

Tartu Ülikool
Sotsiaalteaduskond
Ajakirjanduse ja kommunikatsiooni osakond

ARVUTI- JA INTERNETIKASUTAJATE
KÄITUMINE RISKIÜHISKONNAS
Bakalaureusetöö

Autor: Urmas Rosenberg
Juhendajad: Pille Runnel, MA
Pille Pruulmann-Vengerfeldt, MA

Tartu
2005

Sisukord

Sissejuhatus.....	3
1. Töö teoreetilised ja empiirilised lähtekohad.....	5
1.1. Riski mõiste.....	5
1.2. Riskiühiskonna mõiste.....	10
1.3. Riskikäitumine.....	12
1.4. Arvutitega seotud riskid.....	14
1.5. Internetikasutus Eestis.....	17
1.6. AOL ja NCSA uuring arvutiga seotud probleemide kohta.....	21
2. Uurimisküsimused.....	23
3. Meetodika.....	24
4. Uurimistulemused.....	26
4.1. Hinnangud oma oskustele.....	26
4.1.1. Tarkvara paigaldamine ja kasutamine.....	29
4.1.2. Kogemused viiruste ja rämpspostiga.....	30
4.2. Probleemide lahendamine.....	33
4.2.1. Kes lahendavad probleeme.....	33
4.2.2. Juhendatavad muutuvad juhendajateks.....	34
4.2.3. Lahenduste mudelid.....	35
4.3. Usaldus.....	38
4.3.1. Isiklike andmete edastamine Internetti.....	38
4.3.2. Internetis leiduva info usaldamine ning kasutamine.....	39
4.3.3. Suhtumine kommentaaridesse.....	41
4.4. Info hankimine meediast arvutitega seotud probleemide kohta.....	43
Järeldused ja diskussioon.....	48
Kokkuvõte.....	53
Summary.....	56
Kasutatud kirjandus.....	58
Lisa 1 – Internetikasutajate intervjuu kava.....	59
Lisa 2 – Intervjuude läbiviimise tabel.....	66
Lisa 3 – Eesti Päevalehe ja Postimehe monitooring perioodil 01.01.05 – 28.02.05.....	67

Sissejuhatus

Seoses ühiskonna arenemisega ja aina uute tehnoloogiate kasutuselevõtuga on laienenud ka riskiühiskonna mõiste. Kui varem käsitleti riskidena majanduslikke kriise, looduskatastroofe ning inimese poolt tekitatud õnnetusi, siis tänapäeval on mastaapsed riskid mitte enam indiviidist kaugemale jäävad, vaid ohustavad lausa koduseinte vahel ja isiklike tehnoloogiliste abivahendite kaudu.

Mobiiltelefonid on küll kasulikud abivahendid ning aitavad tänases, paljuski kiirusele üles ehitatud ühiskonnas eluga sammu pidada, kuid samas ohustavad need ka indiviidi julgeolekut ja tema privaatsust. Samamoodi on ka arvutite ja Internetiga, mis arenevad väga kiiresti, kuid sama kiiresti arenevad paralleelselt ka nendega seotud ohud – viirused, nuhkvara, rämpsikirjade saatmine, üldine küberkuritegevus jne.

Et tehnoloogilistes arengutes nähakse autori arvates siiski enam positiivseid külgi, kui ohtusid, siis on tavainimesed neist ohtudest ka vähem teadlikud või, kui ollakse teadlikud, siis ei pöörata neile sedavõrd tähelepanu ning ei peeta olulisteks, vähemalt mitte sinnamaani, kuni need otseselt inimest ennast ei puuduta ja talle endale isiklikku kahju ei tekita.

Käesoleva bakalaureusetöö fookuses ongi arvutikasutajate käitumine seoses arvutitest ning Internetist tulenevate ohtudega ning nende ohtude seostamine riskiühiskonnaga. Ohtudest pööratakse rohkem tähelepanu rämpsikirjadele, viirustele ning isiklike andmete turvalisusele.

Töö teema valiku ajendas eelkõige autori tihe kokkupuude arvuti- ning Internetiprobleemidega ning sellest tulenev huvi uurida neid probleeme lähemalt, nii praktilisest kui teoreetilisest vaatenurgast. Tartu Ülikooli ajakirjanduse ja kommunikatsiooni osakonnas ei ole sellist temaatikat bakalaureuse ega magistritöös varem lähemalt käsitletud.

Bakalaureusetöös keskendutakse arvuti- ja internetikasutajate käitumisele lähtudes riskiteooriast. Kuidas hinnatakse oma oskusi teiste kasutajatega võrreldes? Kuidas

lahendatakse arvuti ja Internetiga seotud probleeme ja kes neid lahendab? Milline on kasutajate usaldus Interneti vastu? Kuivõrd tutvutakse meedias avaldatud arvutite ja Internetiga seotud ohtude teemast kirjutatud artiklitega?

Töö teoreetilises osas käsitletakse riske, riskiühiskonda, käitumist riskiühiskonnas ning arvutiga seotud riske. Samuti antakse ülevaade Internetikasutusest Eestis ning tuuakse võrdluseks välja Ameerikas läbi viidud uuringu andmed, kus vaadeldakse arvutikasutajate arvamusi arvutiga seotud probleemide kohta ning kõrvutatakse neid reaalse olukorraga. Empiirilises osas antakse ülevaade intervjuude tulemustest. Seejärel tehakse järeldused ning arutletakse saadud tulemuste üle riskiteoreetilisest vaatenurgast. Töö lõpetavad eesti ja inglise keelne kokkuvõte ja kasutatud kirjanduse loetelu. Lisadena on toodud intervjuude läbiviimisel kasutatud küsimustik, intervjuude koondtabel ning kahe päevalehe monitooringu koondtabel.

Käesoleva bakalaureusetöö valmimisele kaasaaitamise eest tänab autor oma juhendajaid, Pille Runnelit (kes lisaks juhendamisele aitas ka vahepeal kadumaläinud sihi taasleida) ja Pille Pruulmann-Vengerfeldt'i. Autor tänab ka lähedasi, kes töö valmimisele jõu ja nõuga kaasa aitasid.

1. Töö teoreetilised ja empiirilised lähtekohad

Järgnevas töös osas tuuakse välja teoreetiline lähenemine riskile ning riskiühiskonnale. Kuidas defineeritakse riski ning käitumist läbi selle? Kuna enamasti räägitakse riskidest ning riskikäitumisest seoses loodusega, siis püütakse teoreetilistele käsitlustele tuginedes leida seoseid infoühiskonnaga. Välja tuuakse ka arvutitega seotud riskid, mis sobivad paremini antud töö konteksti ning Interneti kasutajate üldisloomustus, mis näitab kui suurt osa inimestest Eestis antud temaatika puudutab. Teoreetilisele osale järgneb Ameerikas läbiviidud uuringu kokkuvõte, mis illustreerib autori arvates hästi lõhet arvuti- ja Internetikasutajate arvamuste ning reaalse olukorra vahel, tõestades sellega mitteriskiteadlikku käitumist. Viimatimainitud uuringule sarnast Eestis läbi viidud ei ole.

1.1. Riski mõiste

Ulrich Beck (1992) on öelnud, et riskid ei ole modernse ühiskonna leiutis, et kõik, kes on maid avastanud, nagu Kolumbus, on riske tunnetanud. Kuid siis vaadeldi pigem personaalseid riske, mitte globaalseid, nagu tuumaenergia või radioaktiivsete jäätmete ladestamine. Varem vihjas sõna "risk" vaprusse või seiklusele, mitte aga enese või kogu elu hävinemise ohule (Beck 1992:21).

Risk eeldab ohtu, mitte kindlasti sellest teadlik olemist. Isik, kes riskib, kutsub esile ohu, mida mõistetakse kui ähvardust soovitud tulemusele. Igaüks, kes võtab riski, on teadlik ohust, mis võib antud tegevusega kaasneda. Kuid kindlasti on võimalik ka tegutseda nii, et isikud, kes selles osalevad, ei tea kui riskantne see on (Giddens 1990:34-35).

Riski mõiste on seotud moderniseerumise mõistega. **Riski võib defineerida kui süstemaatilist viisi tegelemaks ohtude ja ebaturvalisustega**, mis on tekitatud moderniseerumise käigus/poolt. Riskid, varasemate ohtude vastandid, on moderniseerumise ning globaliseerumise ähvardavate jõududega seotud tagajärjed (Beck 1992:21).

Antud definitsiooni peab autor käesoleva töö fookust silmas pidades kõige olulisemaks, sest tegutsedes vastu arvuteid ähvardavatele ohtudele, vähendavad inividid nende ohtudega kokkupuutumise võimalust. Sellest definitsioonist saab välja lugeda ka olulise vajaduse – nimelt tänu suunatusele tulevikku, on meil vaja infot riski kohta. Ehk, teadmiseta ohtudest, ei saa ka olla riski.

Risk on muutunud elu juhtimise vahendiks, võimaldades inimestel hinnata võimalikke tagajärgi. Ka Giddens (1999:3) on öelnud, et risk viitab võimalusele vältida soovimatuid tagajärgi aga viib samas julgemate ettevõtmisteni.

Tänases ühiskonnas määravad paljuski meie käitumise riskid, mille juures on väga oluliseks komponendiks informeeritus – riski ei eksisteeri enne, kui meil on olemas teadmine antud riskiga seotud tagajärgede kohta.

Miski ei ole risk iseenesest, realselt ei ole riske olemas. Samas võib kõik olla risk. Risk ei ole täielikult objektiivne või mõistetav väljaspool uskumiste süsteemi. See, mida mõeldame, identifitseerime ja haldame kui riske, on alati määratud läbi eelteadmiste ning teadaolevate teemade. Kogu teadmine riskide kohta on piiratud sotsiokultuurilise kontekstiga, kus see tekitatakse teadlaste või teiste, mitte-ekspertide, poolt (Lupton 1999:28-29).

Riski ei ole enne, kui on olemas vajalikku infot. See tähendab, et ei ole teadlikkust riskist enne, kui see risk konstrueeritakse või antakse selle kohta infot. Siit edasi on olulisel kohal meid ümbritsevad inimesed ning kõikvõimalik meedia, kust me oma usalduse piires infot hangime, võimaldamaks edaspidi riskiteadlikumalt käituda.

Riski võib käsitleda läbi selliste terminite nagu ignorantsus, ebakindlus, kahemõttelisus, ebaselgus ning mittetäielik teadmine (Shapira 1994 ref. Kendra & George 2001:129). Inimeste tajusid mõjutavad isiklikud uskumused, hoiakud, ignorantsus, väärtused ja mittetäielikud teadmised (Slovic et al. 1980 ref. Kendra & George 2001:129).

Risk sõltub otsustest – see on peegeldus inimeste tegemistest ja tegemata-jätmistest. See tähendab, et ohtude allikad ei ole mitte enam "ignoreerimine", vaid "teadmine", mitte

puudujääk, vaid täielik valitsemine looduse üle, mitte inimese taiplikkus, vaid normide ning piirangute süsteem (Beck 1992:183).

Paljuski määravad tänase ühiskonna käitumise teadlaste etteöeldud reeglid – tehes nii, on kõik korras, tehes teisiti, riskite selliste ja selliste tagajärgedega.

Objektiivsed faktid, mille eksperdid on välja arvutanud, on vastandlikud mitteteadlike inimeste subjektiivsete arusaamistega. Mitte-eksperdid kas üle- või alahindavad riske: ülehindama kiputakse neid riske, mille kohta on võimalik kergesti infot saada ning mida on kerge mõista, aga ka neid riske, mis esinevad harvemini, on füüsiliselt lähedal või mille kohta kujutatakse ette, et see võib juhtuda nende endaga. Samas alahinnatakse riske, mida peetakse üldisteks või vähemtõsisteks (Lupton 1999:19-20).

Kuna tehnoloogia-ajastul elamine on toonud kodudesse palju tava- ja kõrgtehnoloogiat, mis vääral kasutamisel võib muutuda eluohtlikuks, siis tagab nende seadmete kasutamise oskus turvalisema elukeskkonna.

Paljude uute riskide tunnetamine käib inimestele üle jõu. Fookus on järjest enam ja enam ohtudel, mis on ohvrite jaoks nähtamatud ning tunnetamatud. See jätab aga ohvrid täielikult ekspertide hinnangute, vigade ning vaidluste meelevalda (Beck 1992:27).

Riskiga seoses muutub oluliseks ka usaldus, sest võttes vastu otsuseid ning vastutades nende otsuste eest, peab usaldama otsuse vastuvõtmisel kasutatud infot ning selle allikaid.

Luhmann (1988) ütleb, et usaldust tuleb otseselt riskiga seostada. Soovimatud tulemused on tagajärjeks pigem meie endi tegevustele või otsustele, kui looduse varjatud tähendustele. "Risk" asendab seda, mida varem tähendas "fortuna". Usaldus (*trust*) eeldab teadlikkust riski asjaoludest samas kui enesekindlus (*confidence*) mitte. Usaldus (*trust*) ja enesekindlus (*confidence*) viitavad mõlemad ootusele, mida saab kas nurjata või eirata. Luhmanni kasutuses viitab enesekindlus rohkem või vähem enesestmõistetavale käitumisele, et tuttavad asjad jäävad stabiilseks (Luhmann 1988 ref. Giddens 1990:30-31).

Usaldus on seotud teadliku alternatiivide loomisega. Kui keegi ostab vana auto, siis ta riskib pettasaamisega. Ta usaldab müüjat või tema firma reputatsiooni, et püüda pettasaamisest hoiduda. Seega, isik kes ei kaalu alternatiive, on enesekindel, samal ajal kui see, kes kaalub alternatiive ning arvestab riske, usaldab. Isik, kes on enesekindel, süüdistab pettuse korral teisi. Isik, kes on usaldanud, peab aga osaliselt ennast süüdistama ning võib kahetseda kellegi või millegi usaldamise pärast (Luhmann 1988 ref. Giddens 1990:30-31).

Me ei saa usaldada enam digitaalsetest kanalitest pärit infot reaalsuse kohta – pilt, video või heli võib olla tehtud teises kohas, teisel ajal või laboris, pruukimata olla see või sellega seotud, mida meile räägitakse (Van Loon 2002:150)

Van Loon'i mõte iseloomustab väga hästi tänase infoajastu probleemi – kui siiani on inimkond pidanud oma silma kuningaks, siis nüüd, kus tipptasemel infotehnoloogia abil on võimalik luua nii „reaalset“ pilti kui heli, ei saa enam ühegi materjali autentsuses kindel olla. See kehtib nii tõendite, kui ka lihtsalt info kohta – kuidas teada saada, milline info on usaldatav ning milline mitte?

Risk on alati seotud turvalisuse, julgeoleku ning vastutusega (Giddens 1999:7). Turvalisus on enamasti usalduse ning vastuvõetava riski tasakaalupunktis (Giddens 1990:36). Usaldades kindlat objekti, on risk väiksem, samas kui mitteusaldatav objekt toob kaasa suurema riski turvalisusele ning julgeolekule. Sellest tuleneb ka vastutus otsuste ees. Seega on risk seotud teadmistega, olles paremini välditav, juhul, kui omatakse rohkem infot.

Risk ei ole ainult ühe indiviidi käitumise küsimus või probleem. Leidub keskkonna riske, mis mõjutavad suuri rahvamasse või isegi terve maakera elanikke korraga – näiteks ökoloogilised õnnetused või tuumasõda (Giddens 1990:35).

Võrreldes omavahel ökoloogilisi ning infotehnoloogilisi riske ilmneb nende ühise joonena globaalne efekt, ehk see, et nende tagajärjed mõjutavad väga suurt hulka inimesi.

Ohtlikud ja vaenulikud jõud on peidetud ohutute fassaadide taha. Kõike peab vaatama topelt-põhjalikkusega, et seda mõista. Nähtavat maailma tuleb uurida ning mõista läbi selle peidetud maailma. Need, kes lihtsalt kasutavad asju, võtavad neid nii nagu nad on, kes ainult hingavad ja söövad, ilma uurimata asjade (toksilist) tausta, ei ole mitte lihtsalt naiivsed, vaid nad ei mõista neid ohte, mis neid ähvardavad ning jätavad end nende ohtude kätte kaitseta. Ohtude nähtamatus ei ole nende mitteksisteerimise tõestus; kuna nende (ohtude) reaalsus paikneb nähtamatul alal, siis on neil seetõttu lõpmatu mänguruum (Beck 1992:72-73).

Mõned inimesed on riskide levimisest ja nende arvukusest rohkem mõjutatud kui teised. Moderniseerumise riskid tabavad varem või hiljem inimesi, kes neid riske ise toodavad või neist kasu lõikavad. Riskid sisaldavad bumerangi efekti, murdes nii klasside kui rahvuste mustrid. Ökoloogilised õnnetused ja radioaktiivne leke ignoreerivad riigipiire ja rahvuseid. Samuti on nende eest kaitsetud rikkad ja võimu omavad inimesed. Need ei ole ohud mitte ainult tervisele, vaid ka legitiimsusele, omandusele ning kasumlikkusele (Beck 1992:23).

Piiride puudumine kehtib ka tänaste infotehnoloogiliste riskide kohta – arvutiviirused ning küberrünnakud ei tunne riigipiire ning sarnaselt ökoloogiliste riskide bumerangi efektile, jäävad kübermaailmas samuti „õnnetuse“ esilekutsujad ise kannatajateks. Erinevalt ökoloogilistest õnnetustest, kus kaugemal juhtunud õnnetuse tagajärgedel läheb aega, enne kui need meid mõjutama hakkavad, on küberohtude puhul mõju hetkeline, olenemata „allika“ asukohast.

Viiruste, ohtlike programmide ning pettuste hulk, levimise kiirus ning antiviiiruste mahajäämus teeb nende ohtude jälitamise ning algallikate otsimise asjatuks tegevuseks. Fakt on see, et küberriskid võivad levida ühest maailma otsast teise hoolimata riigipiiridest (Van Loon 2002:160).

Küberriskide alla paneb Lupton viirused (ülemaailmne süsteemide hävitamine), ähvardavad ohud (Y2k probleem, sellest räägiti aastaid, kuid lõpuks ei juhtunud midagi), sõltuvused (mängud, jututoad, pornograafia). Filmides on tihti riske seostatud tehisintellektiga, luues vaatajate peas pildi ohtlikust leiutisest (Van Loon 2002:161-165).

1.2. Riskiühiskonna mõiste

Kui industriaalühiskonnas mõjutasid inimeste käitumist eelkõige sotsiaalne taust ning loodusliku hävinguga seotud probleemid, siis modernses ühiskonnas on oluline toimetulek tehnoloogilist laadi probleemidega.

Moodsat maailma on pikka aega kujundanud teadus ja teaduslikud avastused. Arengu kiirenedes murravad uued tehnoloogiad üha rohkem ja rohkem meie ellu ning üha rohkem on kõik, mida tunneme või kogeme, seotud teadusega (Giddens 1999:1).

Kui industriaalühiskonnas oli "väline risk", mis oli seotud looduse ning väliste jõududega, siis riskiühiskonnas on "toodetud risk", mis luuakse teaduse ning tehnoloogia kaudu (Giddens 1999:4).

Industriaalühiskonnas pidi iga inimene võitlema materiaalse vaesuse ning sotsiaalse allakäigu vastu – see oli kogu elu keskseks teemaks nii ühiskonna kui indiviidi tasandil. Riskiühiskonnas muutuvad aga elutähtsaks lisaoskused – olulised on ohtude ennetamine ning nende suhtes vastu pidamine. Staatuse kaotuse, klassiteadlikkuse ning klassiredelil ülespoole liikumise probleemide asemele on tulnud uued kesksed küsimused: kuidas tulla toime hirmudega, kui me ei saa toime tulla nende hirmude põhjustega. Riskiühiskonnas muutub oluliseks toimetulek hirmude ning ebaturvalisusega ning vajalike teadmiste ja kogemuste jagamine jääb pedagoogiliste asutuste missiooniks (Beck 1992:76).

Giddens toob näiteks Simon Sebag Montefiore seletuse Nick Leesoni ja Barrings'i panga kohta. Sebag Montefiore pakub, et tegu oli korruptsiooni ning kahtlase juhtimisega. Samas ta siiski kahtleb selles ning pakub hoopis välja modernse ajastu seletuse: "Inimesed, kes töötavad rahandusturgude viimaste piiride peal, on kui astronautid. Nad on astunud pankurite ning rahandusekspertide alalt (*realm*) välja. Kui ülejäänud (kosmonaudid) on jäänud ühendatuks kapsli külge, siis Nick Leeson läks liiga kaugemale. Ehk siis – nad on seotud süsteemidega, mida nad isegi ei tunne, nii äärmuslik on muutuste pealetung uues globaalses elektroonilises majanduses. Selliste äärmuslike piiride peal oleme täna me kõik." Ulrich Beck nimetab seda riskiühiskonnaks. Riskiühiskond on ühiskond, kus elatakse üha rohkem kõrgtehnoloogilisel piiril, mida

mitte keegi enam täielikult ei mõista (1999:2-3).

Levib arusaamine, et rikkuse allikad on saastatud ohtlike kõrvalmõjudega. See ei ole midagi uut, see on lihtsalt jäänud aja jooksul märkamata. Tume külg kogub tähtsust ka tootlike jõudude ülearendamises. Moderniseerumise protsessis päästetakse üha enam valla hävitavaid jõude (Beck 1992:20).

Globaliseerumine toob kannatused, mis on suuremalt jaolt üldised. Kui kõik muutub ohuks, tuleb välja, et miski ei ole enam ohtlik. Kui väljapääsu enam ei ole, loobuvad inimesed ohtudele mõtlemisest. Riskiühiskond nihkub seega hüsteeriast ükskõiksusesse (ja vastupidi). Tegutsemine kuulub ju eilsesse (Beck 1992:37).

Tajumatute riskide ignoreerimine, mille vastu tõeliselt tegutsemist saab alati õigustada, on kultuuriline ning poliitiline pinnas, millel riskid ning ohud kasvavad, õitsevad ning vohavad. Tööstus- ning turuühiskonnas võidab ikka rikkuse ning jõukuse loogika ning see on põhjuseks, miks riskiühiskond on nii võidukas (Beck 1992:45).

Riski tuleb eristada hädaohust. Termin 'riskiühiskond' võib viidata endisest ohtlikumale ühiskonnale, kuid see ei ole nii. Pigem on selline ühiskond mõttesse vajunud tuleviku ning turvalisuse teemadel ning see loobki riski (Giddens 1999:3).

Riskiühiskonna positiivseks küljeks on valikute suurenemine (Giddens 1999:5).

Van Loon (2002) seob Ulrich Beck'i riskiühiskonna analüüsi info- ja kommunikatsioonitehnoloogiatega. Näidetena ühistest joontest toob ta välja moraalse paanika (*moral panic*), loogiliselt mitteseletatava hirmu pärast kindlaid saateid, info ülekülluse ning müra, küberohvrid ning küberkultuurid (milles osalemine võib lõppeda massienesetapuga), häkkimise ning küberpettused. Ja loomulikult, on nende küberriskide krooniks arvutiviirus (2002:158).

Info üleküllust ning müra võib igati pidada Internetiga seotud ohuks. Probleemiks on olulise info väljasõelumine ebaolulise või väärinfo seest. Nimelt on infoühiskonna ning Internetiga seoses tekkinud täiesti uus viis inimeste ründamiseks – pettus, narritamine

(*hoax*). Viimane seisneb adekvaatse välimuse ning täiesti tõepärasena tunduva sisuga kirja või teate saatmises, milles on väärad käitumisjuhendid (Norra viirus, pangakoodide pettused, jne). Arvutikasutaja, kes ei ole nendest temadest teadlik, ei suuda selliseid kirju enam eristada tõelistest õpetustest ning langeb antud väärdõpetuse ohvriks.

1.3. Riskikäitumine

"Tervise uskumuse mudel" (*health belief model*) näitab inimese käitumist kui tahtlikku ning ratsionaalset, mis alati kategoriseerib riski vältimist kui ratsionaalset ning riski võtmist kui irratsionaalset käitumist (Bloor 1995: ptk 5 ref. Lupton 1999:21 kaudu). Vastavalt sellele mudelile peab inimene mõistma mitmeid asju enne, kui ta astub samme enese kaitseks. Inimesed peavad nägema end ohustatuna nendest ohtudest, tajuma, et ohul on tõsised tagajärjed. Nad peavad uskuma, et preventiivsed tegevused on efektiivsed ning et kasu, mis sellest saadakse, on suurem kui kulutused (Lupton 1999:21).

Riski või riskide eksisteerimise äratundmise juures ei ole oluline mitte ainult mõistmine, et asjad võivad valesti minna, vaid et seda võimalust ei saa elimineerida (Giddens 1990:111).

Turvatunde suurendamise asemel on tehnoloogilised süsteemid viinud meid hoopis selleni, et suurenenud on riskitundlikkus. Tänapäeva inimesed ei tunne ülekoormatust täieliku riskiinfo üle, mis käib nende igapäevase elu kohta. See võib aga tekitada nurjumise tunde: info üleküllus muudab ratsionaalse käitumise riskide suhtes peaaegu võimatuks. Kui see panna kokku individualiseerumisega, kus järjest rohkem ja rohkem olulisi otsuseid on lükatud indiviidi enda vastutusele, muutub üha raskemaks ratsionaalsete riskikäitumiste arendamine/loomine. Kui kõik on riskantne, kaotab risk oma tähtsuse (Van Loon 2002:188).

Giddens (1990) ütleb, et **mittetegutsemine on sageli riskantne** (Giddens 1990:32). Infotehnoloogia mõttes on mittetegutsemine riskantne mitmel kujul – esmalt info, mitte juurde hankimine loob tänu uute teadmiste puudumisele olukorra, kus uute probleemidega ei osata ümber käia, ning, teisalt, võimaldab mittetegutsemine juba

toimunud negatiivsete sündmuste tagajärgedel edasi areneda ohustades sellega teisi arvuti- ning Internetikasutajaid.

Riskid ei ammenda ennast loomulikult ainult efektides ja kahjustustes. Tuleb vahet teha "juba hävitusliku tagajärje" ning "potentsiaalset" tüüpi riskidel, kus teisel juhul väljendab risk tulevikku. Seda leitakse praegu teadaoleva kahjuliku mõju jätkamisel tulevikku, üldiste kaotuste või "riskikordajate" kaudu. Sellisel juhul on juba täna reaalseks saamas riskid, mis on seotud vastumeelsuse või kaotustega, mida pole veel läbi elatud, aga mis on hirmutavad. Teisisõnu: aegpomm tiksub. Selles mõttes tähendavad riskid ärahoitud tulevikku (Beck 1992:33).

Riskiteadlikkuse kese ei asu mitte olevikus, vaid tulevikus. Riskiühiskonnas kaotab minevik jõu selleks, et määrata olevik. **Me muutume aktiivseks täna selleks, et leevendada või võtta kasutusele ettevaatusabinõud homsete (ja ülehomsete jne) probleemide ja kriiside vastu** (Beck 1992:34). Looduses, keskkonnas, mis on inimestele tuttav, ei ole probleeme mõistmaks, et tuleb astuda samme homsete probleemide vastu – teades, et vulkaan võib aktiveeruda igal hetkel, kolivad inimesed minema. Infotehnoloogia on aga tänu oma kiirele pealetungile võtnud inimestelt ära võimaluse selle uue keskkonnaga kohaneda ning seega ei pruugita suuta mõista, mil moel midagi käega katsutamatut seotud reaalse eluga.

Riskide globaliseerumine – riskid mõjutavad kõiki või vähemalt väga suurt hulka inimesi (Giddens 1990:124). Seoses riskidega, mis on võimelised mõjutama kogu inimkonna elu, on ära kadunud mõiste "teised": nii võitlejad kui eemalseisjad kannatavad (Giddens 1990:126). See viitab globaalse ühiskonna olemusele, kus ühe käitumine mõjutab kõiki teisi. Inimese kasutatavad tehnoloogiad on muutunud nii võimsaks, et nende poolt tekitatavad võimalikud katastroofid on võimelised mõjutama kogu maakera elanikke.

Kui loodusega seotud riskide mõistes räägitakse näiteks tuumatalvest, kus kannatajateks jäävad lõpuks kõik, siis arvuti ning Interneti osas on olukord sama – saates Internetti uue viiruse, jääb kannatajaks ka viiruse autor ise. Samuti ei ole „teisi“ häkkimisel: „Hiinas murti sisse kellegi arvutisse“ – see ei tähenda, et see on „teiste“ probleem või et me oleme neist kaugel – viis minutit hiljem võib see sama rünnak tabada meid.

1.4. Arvutitega seotud riskid

Internetis ja arvutis paiknevate andmetega seoses eeldavad ning ootavad inimesed teadlikult või mitteteadlikult turvalisust. Kuigi turvalisuse sõna on tuttav ning kõik teavad, mida see igapäevaelus tähendab, on arvuti ning andmete mõistes tegu definitsiooniga, mis koosneb kolmest kategooriast:

1. **Konfidentsiaalsus** (*confidentiality*) – andmed on kättesaadavad ainult autoriseeritud isikutele ja organisatsioonidele.
2. **Terviklikkus** (*integrity*) – andmed on autentsed ning täielikud.
3. **Käideldavus** (*availability*) – süsteem on võimeline andmeid edastama, salvestama ning töötleva kui selleks tekib vajadus.

(Veldre 2003, Neumann 1995:96-97)

Kõike, mis ohustab neid kolme kategooriat, käsitleme kui riske ning kasutusele tuleks võtta vastumeetmed soovimatute tagajärgede ärahoidmiseks.

Konfidentsiaalsuse rikkumine toimub siis, kui privaatsed või salajased andmed satuvad volitamata isikute kätte. Kui kõrvaline isik satub lugema teise inimese haiguslehte, saab kätte firma raamatupidamisandmed või kui kohtuhoone prügikastist leitakse salajased dokumendid – see kõik rikub konfidentsiaalsust. Terviklikkus tähendab seda, et andmed, mida kasutatakse on õiged ning need on täies mahus kättesaadavad. Terviklikkus on rikutud juhul, kui näiteks autoregistris on volituseta muudetud registri andmeid – info saadakse küll kätte, aga see ei vasta enam reaalsusele. Terviklikkuse osa rikutakse siis, kui meile ei võimaldata ligipääsu kogu infole – näiteks jäetakse teadlikult välja autoga seotud õnnetused. Käideldavus on rikutud sellisel juhul, kui puudub mõistlike tingimustega ligipääs andmetele või võimalus nendega tööd teha – näiteks, kui internet on küberrünnaku tagajärjel väga aeglane, serverid ülekoormatud vms.

Võib öelda, et turvalisus on mõjutatav kõikjal seal, kus on arvutid (ka arvutitest väljapoole) – kui arvuti, mis kontrollib ligipääsu büroohoonele, on häkkerite poolt hõivatud, siis võib juhtuda kõike, alustades sellest, et inimesed ei saa tööd teha kuni selleni, et kellegi elu satub ohtu. Arvuti üle kontrolli võtmine häkkerite poolt võib alguse saada tühistest kasutaja tehtud sammudest – kasutaja käib spetsiaalset tarkvara

installeerival kodulehel, käivitab e-kirja manuse, installeerib ettejuhtuva tarkvara, kasutab nõrku paroole ning vana tarkvara jne.

Kolm peamist arvutite ja Internetiga seotud, riski millega inimesed kokku puutuvad ning millele keskendub käesolev töö, on viirused, rämpskirjad ning nuhkvara.

Viirused on programmid, mis levivad iseseisvalt kasutades selleks võrku või teisi programme ning kannavad tihtilugu eneses mingit ülesannet – lihtsalt paljuneda, koguda informatsiooni, kustutada andmeid, avada ligipääs häkkeritele jne. Viirused rikuvad kõiki turvalisuse kategooriaid – konfidentsiaalsust (viirused võivad arvutikasutaja teadmata edastada dokumente), terviklikkust (viirused muudavad või hävitavad peremeesfaile) ning käideldavust (kui arvuti on viirustega nakatunud, siis kõige muu hulgas kannatab arvuti jõudlus). Viirused on risk, mille tagajärgi on võimalik riskiteadliku käitumisega vähendada, mõistes samas, et 100% kaitset luua ei ole võimalik.

Rämpskirjad on soovimatud kirjad, millega edastatakse reklaami või viiteid lehekülgedele, mille kaudu omakorda püütakse nakatada arvutit, edastada reklaami või lihtsalt püüda külastajaid (millega on võimalik raha teenida). Rämpskirjad ise otseselt ei riku konfidentsiaalsust ega terviklikkust sest need on passiivsed objektid. Küll aga võivad need olla vahendajateks viirustele või nuhkvarale. Rämpskirjad rikuvad aga käideldavuse kategooriat, st peame sooritama tööga otseselt mitteseotud lisategevusi selleks, et eemaldada sisuka e-posti seast rämpskirjad ning seega see segab otseselt nii meie kui ka meiliserverite tööd. Rämpskirjadele ei tohiks mittemingil juhul vastata.

Nuhkvara on mõeldud arvutikasutajate tegevuste jälgimiseks. Peamiselt salvestatakse ning edastatakse selle abil „peremehele“ infot Internetis külastatud lehekülgedest. Nuhkvara on kõige ohtlikum konfidentsiaalsuse mõttes. Kuna sellised programmid on võimelised jälgima kõike, mida tehakse – klahvivajutused, programmide käitumine, toimingud avatud akendel, siis on võimalik teada saada kõik, mida kasutaja arvutisse sisestab, sh ka näiteks Internetipanga koodid ning salasõnad. Terviklikkuse osas enamasti nuhkvaraga probleeme ei ole, kuna nende eesmärgiks ei ole muutmine vaid kogumine. Käideldavuse kategooria rikkumise mõttes on probleem olemas, aga mitte nii tõsiselt kui viiruste ning rämpskirjadega, kuna enamasti ei levi need kontrollimatult omapäi.

Kõiki arvuti ja Internetiga seotud probleeme ei ole võimalik siinkohal üles loetleda. Alljärgnevalt tuuakse välja veel mõned riskid lisaks eelmainitutele, mis on olulisemad ning mille suhtes saaksid inimesed ka ise midagi ette võtta:

- Tarkvara uuendused – tihtilugu leitakse tarkvarast turvaauke ning sellisel juhul annab vana versiooni kasutamine suurema võimalus häkkeritele arvutisse sisse murda, lisada oma tarkvara vms, ent nagu on ka öelnud Alberts & Dorofee (1992:xxv) et ei tohiks loota, et uue tarkvara paigaldamine lahendab kõik probleemid.
- Tarkvara andmete uuendused – eriti puudutab see viirustõrjeid, tulemüüre ning rämpspostifiltreid – kui andmed on uuendamata, siis ei tunta uusi viiruseid ning rünnakuid ära ning tulemuseks on petlik turvatunne.
- Tundmatu päritoluga andmefailide avamine – võivad sisaldada viiruseid (e-kirja manustena enamasti) või kasutada ära tarkvara turvaauke ning sealtkaudu omandada kontrolli arvuti üle.
- Võõraste väliste andmekandjate (disketid, USB pulgad jne) ning nendel olevate andmete ja programmide kontrollimata kasutamine.
- Arvuti kasutamine administraatori õigustes – kui kasutaja käivitab kahtlase programmi või tema poolt avatud andmefail viib ründeprogrammi käivitamiseni, siis saab kahjustada kogu süsteem ning seeläbi ka kõik teised kasutajad selles arvutis. Kui kasutaja on süsteemi sisse loginud oma õigustes, üldiselt kahjustada ainult tema enda andmed ja programmid.
- Interneti protokollide kasutamine – kuna enimkasutatavad protokollid ning kanalid nagu http, ftp, telnet, msn jne ei ole krüpteeritud¹, siis on kõik info kõigile nähtav ning loetav – seega tuleks hoiduda igasuguse personaalset ja konfidentsiaalset laadi info edastamisest internetti selliste kanalite kaudu.
- Ilma tulemüürita Internetti ühendumine – tulemüür on tõkkeks välisvõrgust tulevate rünnakute ja ohtude vastu. Kasutades tulemüüri ning sulgedes välisvõrgu jaoks kõik mittevajalikud ühendused vähendame riske, et häkkerid suudaksid arvutisse sisse tungida. Samuti aitavad tulemüürid vältida soovimatuid ühendusi sisevõrgust väljapoole – ebasoovitavate Internetilehtede külastamine, viiruste ning nuhkvara ühendused „peremeesteni“ jne. Tulemüürid aitavad ka vähendada võimalust, et antud arvutit või arvutivõrku saaks kasutada hüppelauana järgmistele rünnakutele.

¹ Faili krüpteerimise eesmärgiks on muuta failis asuvad andmed võõrastele loetamatuteks ehk teisisõnu öeldes info salastada (<http://www.id.ee/pages.php/03020702,734>).

- Seadistuste vead – kui muidu turvaline süsteem seadistada valesti, siis võime tekitada sellega väga suure turvaprobleemi mis võib lõppeda kõigega, alates sellest et häkkerid saavutavad arvuti üle kontrolli, kuni selleni, et kaduma lähevad kõik andmed.
- *Social engineering* ehk käitumine kus inimene meelitatakse oma paroole avaldama jättes endast mulje kui süsteemiadministraatorist või näiteks küsides asju justkui läbi viies uuringut.
- Tagavarakoopiate puudumine – arvutustehnikale võivad saada saatuslikuks kõikvõimalikud ohud – vesi, tuli, elekter, vandalism, loodusõnnetus, häkkerid – ning koos sellega võivad kaduma minna ka kõik olulised andmed. Seda riski saab vähendada, kui tehakse regulaarselt koopiaid ning säilitatakse neid füüsiliselt erinevas kohas.
- Keerulisemateks probleemideks võib lugeda võrguga seotud probleeme nagu DNS mürgitamine, IP ning MAC aadressi vahetus ja võltsimine, ühenduste kaaperdamine, võrguliikluse suunamise võltsimine.

Lisaks otsesele ohule arvuti- ja Internetikasutaja andmetele, programmidele ning arvutitele võivad arvutitega seotud riskid mõjutada ka meie mainet – rämpsposti saatmine meie võrgust häkkerite poolt, veebilehe näotustamine või rünnakud meie partnerite vastu viivad usalduse kaotamiseni.

Mida rohkem inimesi kasutab arvutit ja Interneti, seda suurem on oht, keegi neist satub küberriskist tulenevate tagajärgede ohvriks. Kuna Eesti on arvutite ning Interneti kasutuse poolest küllaltki kõrgel tasemel, siis puudutab see otseselt ka meid.

1.5. Internetikasutus Eestis

Eestis kasutab viimase Emori (2005) uuringu järgi Interneti ning arvuteid 51% 15-74-aastastest eesti elanikest – see on suur hulk inimesi, kes puutub päevast päeva kokku Internetist tulevate ohtudega. Järgnevalt toob autor välja ülevaate Eesti Internetikasutajatest, nende põhitegevustest ning hinnangutest oma oskustele ning Internetist tulenevatele ohtudele.

Internet on pärisnimi, mis tähistab ülemaailmset arvutivõrgustikku, mis töötab TCP/IP protokollil. Väikese tähega kirjutatult tähistab "internet" aga erinevaid ülemaailmseid arvutivõrke (Vengerfeldt & Runnel 2004:233).

Kommunikatsiooniteaduslikust vaatepunktist on Internet erilaadsete kommunikatsioonikanalite mitmekülgne kogum ja multimediaalne publitseerimisvahend, mis võimaldab edastada või vahetada nii tekstilist, helilist kui ka pildilist infot. Interneti osaks on nii staatilise ülesehitusega visuaalset ja tekstilist infot kombineerivad veebiküljed kui ka reaajas toimuv multimediatseeritud otsesuhtlus kahe inimese või paljude eri osavõtjate vahel (Vengerfeldt & Runnel 2004:233).

Eesti Interneti alguseks võib lugeda 26. märtsi 1992, sest siis käivitus esimene TCP/IP ühendus Eesti ja muu maailma vahel. TA Keemilise ja Bioloogilise Füüsika Instituudi ja Rootsi Kuningliku Tehnikaülikooli vahel pandi tööle 64kbit/s satelliidiühendus (Vengerfeldt & Runnel 2004:235).

Andmed Eesti Internetikasutuse kohta pärinevad Tartu Ülikooli ajakirjanduse ja kommunikatsiooni osakonna uurimusest (MeeMa), mis viidi läbi 1. detsembrist 2002 kuni 6. jaanuarini 2003, hõlmates esinduslikult 15-74aastast Eesti elanikkonda.

Küsitluse toimumise ajal kasutas Eestis arvutit 48% elanikkonnast. Kodudes oli arvuti olemas 38% elanikkonnast (Runnel & Pruulmann-Vengerfeldt 2004:148).

Vanuserühmade lõikes kasutati arvutit kõige rohkem 15-19aastaste rühmas – tervelt 88%. Edasi hakkab kasutusprotsent langema, olles 20-29aastaste rühma juures 72 ning kahanedes lõpuks 65-74aastaste rühma juures 9 protsendini. Arvuti kasutamise erinevust on näha ka sissetulekute lõikes – peres, kus sissetulek pereliikme kohta oli kuni 1500 krooni, kasutati arvutit 38% ning peres, kus sissetulek pereliikme kohta oli üle 6000 krooni kasutati arvutit 82.5%. Kõige enam kasutati arvutit, kas tööl või koolis, kus praktiliselt iga päev kasutab arvutit 65% arvutikasutajatest (Runnel & Pruulmann-Vengerfeldt 2004:149-151).

Peamiselt kasutati arvutit Internetist info otsimiseks ning e-kirjade saatmiseks, aga ka veel väga palju tekstitöötamiseks. Tüüpide järgi jaotub kasutus järgmiselt: kontoritarkvara ja Interneti kasutaja (38% arvutikasutajatest), vähekasutajad (22% arvutikasutajatest), arvutikasutajad erialaseks tööks (17% arvutikasutajatest), aktiivsed ja mitmekülgsed mängijad (13% arvutikasutajatest) ning lõpuks kontoritarkvara kasutajad (6% arvutikasutajatest) (Runnel & Pruulmann-Vengerfeldt 2004:152-153).

Interneti kasutas kõigist uuringus osalenutest 43%. Vanuserühmade lõikes vaadatuna oli kasutuspilt sarnane. Kõige rohkem Internetikasutajaid oli 15-19aastaste rühmas – 85%, sealt edasi rühmade kaupa kasutus langeb, jõudes 65-74aastaste rühma juures 4.5% juurde. Samuti on Internetikasutus väiksem rühmas, kus kuusissetulek inimese kohta on kuni 1500 krooni (30%) ning suurim selles rühmas, kus sissetulek on inimese kohta üle 6000 krooni (79%) (Runnel & Pruulmann-Vengerfeldt 2004:154-155).

Hinnangutes oma arvutikasutusoskuste kohta arwab 39%, et nende tase on rahuldav. 29% peab seda heaks ning 9% väga heaks. Kõige enam hindavad oma oskusi väga heaks üle 6000-kroonise sissetulekuga inimesed (19%), kõrgema haridusega inimesed (13%), 20-29-aastased (12%) ning mehed (12%). Kasutajaid kes arvavad, et nad ei oska peaaegu üldse arvutit kasutada on 3% ning vähese oskusega kasutajaid on 20% (Runnel & Pruulmann-Vengerfeldt 2004:153-154).

Arvamuse avaldamise kohana, hinnatuna viiepalli skaalal, peavad vastajaks kõige olulisemaks avaliku arvamuse uuringuid (keskmine 3.84), telesaadetes osalemist (keskmine 3.67) ning lugejakirju (keskmine 3.61). *On-line* portaalides kommenteerimine (keskmine 3.17) on üks vähemolulisemaid jäädes nimekirja lõppu koos meililistidega (keskmine 2.92) (Runnel & Pruulmann-Vengerfeldt 2004:160-161).

Ohufaktoriga tunnetati kõige rohkem seost selliste hoiakutega nagu "Lapsed saavad Internetist neile sobimatut informatsiooni", "Arvutite ja Interneti sage kasutamine on tervisele kahjulik" ning "Internet soodustab tarbetut ajaraiskamist". Hirmu osas kujunesid välja kõige enam seosed hoiakutega "Arvutite ja Interneti kasutamine hirmutab mind" ning "Interneti tõttu võõranduvad inimesed üksteisest" (Runnel & Pruulmann-Vengerfeldt 2004:159-160).

MeeMa uuringu põhjal jaotati vastavalt Interneti kasutuse aktiivsusele ning tegevuse orienteeritusele kasutajad kuude gruppi:

1. Vähekasutaja (20% internetikasutajatest) – väheaktiivne suhe Internetiga ja kindlate kasutuseelistuste puudumine.
2. Eraeluliste teenuste kasutaja (15% internetikasutajatest) – orienteeritud mitmekesise info saamisele, peamiselt eluaseme, töö ja reisimisega seotud info.
3. Virtuaalses avalikkuses osaleja (18% internetikasutajatest) – orienteeritud jututubades ja foorumites osalemisele, kommentaaride lugemisele ja kirjutamisele.
4. Suhtleja (17% internetikasutajatest) – suhtlus on kõige olulisem.
5. Mitmekülgne interaktiivne võrgusolija (15% internetikasutajatest) – nende jaoks on Internet ennekõike keskkond. Kesksel kohal on suhtlemine ja praktilise info saamine.
6. Mitmekülgne infokasutaja (16% internetikasutajatest) – Interneti kasutamisel on oluline erialane ja õppimisega seonduv info.

(Vengerfeldt & Runnel 2004:253-254).

Praktiliselt iga päev kasutasid kodus keskkonnas Internetti need, kelle jaoks see oli info hankimiseks, osalemiseks või suhtlemiseks (vastavalt VI, III ja IV tüüp), eriti aga need, kelle võrk oli interaktiivne ümbritsev keskkond (II tüüp - 80% kasutas Internetti kodus praktiliselt iga päev). Tööl ja koolis olid teistest märgatavalt aktiivsemad mitmekülgset infokasutajad (VI tüüp), kellest 87% kasutas Internetti praktiliselt iga päev. Kodune kasutus on teisest sagedasem suhtlejatel (IV tüüp) ning mitmekülgsetel infokasutajatel (V tüüp) (Vengerfeldt & Runnel 2004:254).

Internet on Eestis olnud ligi kolmteist aastat ning selle aja jooksul on seda kasutama hakanud pool elanikkonnast. Seda võib pidada väga kiireks arenguks, kusjuures selle juures jääb kannatajaks pooleks kasutajate oskuste areng - Internetikasutajatest üle poolte peavad oma kogemusi keskmiseks või nõrgemaks, millest võib ka tuletada, et väga suur osa Eesti Internetikasutajatest on kergemini haavatavad Internetist tulenevate ohtude poolt.

1.6. AOL ja NCSA uuring arvutiga seotud probleemide kohta

Kui küsida Interneti ja arvutikasutaja käest kuidas ta hindab oma oskusi või teadmisi arvutite ja Interneti osas, siis suur osa vastab „keskmine“, ent sellist vastust on väga raske edaspidi kasutada. Sisuka vastuse saamiseks on tunduvalt efektiivsem kõrvutada kasutajate vastus reaalse olukorraga.

2004. aastal viisid AOL ja NCSA Ameerika Ühendriikides läbi uuringu, kus osales kokku 329 Interneti kasutajat vanuses vähemalt 18 aastat. Uuringus osalenud olid pärit 22st linnast, mitmest erinevast osariigist. Uuring koosnes kahest osast – intervjuud ning arvutitestid. Antud töö jaoks võib seda uuringut oluliseks pidada sellepärast, et see uurides inimeste arvamust, kõrvutab need arvamused reaalse situatsiooniga kasutaja arvutis. Eestis samalaadseid uuringuid teadaolevalt läbiviidud ei ole.

77% osalenutest arvasid, et nende arvuti on kas hästi või väga hästi kaitstud Internetist tulevate rünnakute vastu. Samuti arvas ka 73% osalenutest, et nende arvuti on kaitstud viiruste vastu. Otsesest arvutite kontrollist aga selgus, et 19% kasutajate arvutid on nakatunud ühe või enama viirusega, samas kui 96% ei osanud öelda, kas arvutis on viirus, või olid kindlad, et viirust ei ole. Viirustest tuleneva ohu äramärgimiseks on veel hea ära mainida, et suurim viiruste arv, mis ühest arvutist leiti oli 213 (AOL/NCSA 2004).

85% kasutajatest küll omas antiviruse tarkvara, kuid neist ainult 33% olid seda uuendanud viimase nädala jooksul. Kokku üle kõigi osalenute oli 67% selliseid, kellel ei olnud antiviruse tarkvara või polnud seda viimase nädala jooksul uuendanud (AOL/NCSA 2004).

47% uuringus osalenutest arvas, et neil ei ole arvutis nuhkvara, ent kontrollimisel selgus, et 80% kasutajate arvutites oli see olemas. Keskmiselt oli ühes arvutis 93 nuhkvara komponenti. Pärast testimist küsiti kasutajate käest, kas nad olid teadlikud selliste programmide olemasolust nende arvutis ning 89% vastas eitavalt (AOL/NCSA 2004).

Pärast nuhkvara otsimise teste küsiti kasutajatelt, kas nad teavad, mida need programmid teevad ning kuidas neid eemaldada? Vastuseks saadi eitused vastavalt 90% ja 76% (AOL/NCSA 2004).

Testimisel selgus, et 67% kasutajatest ei kasuta tulemüüri (Nende seast, kellel see oli isegi installeeritud, ei töötanud see korralikult 72% juhtudest) (AOL/NCSA 2004).

Kokkuvõtvalt võib kasutajate arvamusi ning arvutite seisukorda võrreldes öelda, et peetakse oma arvutit küll kaitstuks viiruste ja rünnakute vastu, kuid reaalne olukord viitab pigem olukorra tõsidusele, kuna arvutites on juba soovimatud programmid või on kaitseprogrammide kasutamine puudulik – 19% osalenutel oli arvutis viirus, 80% osalenutel oli arvutis nuhkvara ning 67% osalenutest ei kasutanud tulemüüri.

2. Uurimisküsimused

Alljärgnevalt selgitatakse töö eesmärgi ning tuuakse ära uurimisküsimused.

Töö ülesanne on uurida arvuti- ning Internetikasutajate käitumist riskiühiskonnas

2.1. Kuidas hindavad arvutikasutajad ise oma oskusi?

Milline on üldhinnang teiste kasutajatega võrreldes ning kui oskuslikud on tarkvara seadistamisel?

2.2. Kuidas lahendatakse arvutite ja interneti kasutamisel ette tulevaid probleeme?

Antud uurimisküsimuse eesmärgiks on selgitada, kuidas saab arvutite ja Interneti kasutamisel tekkinud probleem lahenduse indiviidi tasandil. Kas probleemiga püütakse ise hakkama saada või jäetakse see kellegi teise lahendada? Kuidas tullakse toime sagedamini ettetulevate probleemidega nagu viirused ja rämspost?

2.3. Kuivõrd usaldatakse internetikeskkonda?

Antud uurimisküsimus aitab selgitada, kas inimesed võtavad enesele suuri riske seoses arvutite ja Internetiga. Kuivõrd usaldatakse seda infot, mis tuleb internetist ning tegutsetakse selle järgi? Kas ollakse valmis isiklikku infot Internetti andma, riskides seeläbi privaatsuse kaotusega?

2.4. Kuivõrd ollakse teadlikud Internetiga seotud ohtudest?

See uurimisküsimus keskendub sellele, mil moel käituvad inimesed lähtuvalt riskidest. Kas otsuste tegemisel teadvustatakse riske, või on tegemist pigem sisseharjunud käitumisega? Kas riskidega mitteamvestamist põhjustab rohkem teadmatus või asjaolu, et läbi arvuti ei ole midagi kaotada? Kui palju meediast arvutite ja Internetiga seotud ohtude kohta infot uuritakse?

3. Meetodika

Käesoleva bakalaureusetöö uurimismeetodiks on kvalitatiivintervjuud.

Ühisuuringu eesmärgiks oli uurida inimeste Internetikasutamise harjumusi, viise ja eesmärke. Käesoleva bakalaureusetöö fookuses on arvutikasutajate käitumine seoses arvutitest ning Internetist tulenevate ohtudega.

Intervjuu valimiks olid inimesed, kes osalesid Tartu Ülikooli ajakirjanduse ja kommunikatsiooni osakonna poolt 2002. aastal läbi viidud uuringus Mina.Maailm.Meedia (Meema) ning kes andsid nõusoleku ka edaspidi küsimustele vastata.

Nende seast valisiti esimeses ringis välja vastajad järgmiste kriteeriumite alusel:

- eesti keelt kõnelevad
- Tartus elavad
- Interneti kasutajad
- nõus intervjuud andma

Selle tulemusel saime kokku 15 vastajat, kellest intervjuud lepidi kokku 11 inimesega, kusjuures ülekaalus olid mehed. Kuna 2 vastajat ei ilmunud kohale, siis Tartus tehti kokku 9 intervjuud.

Teises ringis valisime juurde vastajad järgmiste kriteeriumite alusel:

- eesti keelt kõnelevad
- Tallinnas elavad
- Interneti kasutajad
- nõus intervjuud andma
- naised

Selle tulemusel saime lisaks 18 vastajat, kellest valiti välja 6 esimest ning kõigiga viidi läbi intervjuud. Ajad leppis vastajatega kokku uuringufirma Faktum.

Küsimustik koostati ühiselt nelja tudengi koostöös ning juhendajate Pille Pruulmann-Vengerfeldti ja Pille Runneli juhendamisel. Küsimustik sisaldas erinevaid küsimuste

blokke olenevalt kõigi osalenute uurimisülesannetest, seega sai kokkuvõttes igaüks analüüsida kõikide poolt läbiviidud intervjuude tulemusi. Intervjuu küsimused on ära toodud käesoleva töö Lisas 1. Intervjuudes liiguti üksikult üldisele, inimeste isiklikelt kogemustelt üle üldisemale tasandile.

Pilootuuringu vormis vaadeldi võrdlevalt ka kahte suuremat päevalehte, Eesti Päevalehte ja Postimeest selgitamaks kui palju arvutite ja Internetiga seotud ohtudest kirjutatakse. Valimisse sattusid kogu perioodi jooksul ilmunud tehnoloogiateemalised artiklid, mille kohta märgiti üles artikli ilmumise kuupäev, vorm, maht, lehekülg, pealkiri ja lühike kommentaar sisu kohta.

Intervjuu struktuur

Intervjuude käigus uuriti järgmisi valdkondi:

- I Sotsiaalne võrgustik, kodu, sõbrad, õppimine, töö, huvid ja harrastused
- II Arvutid ja Internet: Kogemused, ootused, harjumused, hüved, hoiakud, motivatsioon
- III Internet ja sotsiaalne võrgustik, suhtlemine
- IV Info otsimine
- V Tarkvara ja riistvara: hirmud, oskused
- VI Info ja kommunikatsioon, infoühiskond (mõiste tähendus, kokkupuude sellega)

Käesoleva töö raames olulised küsimused jaotusid kõigi valdkondade vahel väljaarvatud kolmas valdkond (Internet ja sotsiaalne võrgustik, suhtlemine).

4. Uurimistulemused

Alljärgnevalt tuuakse ära intervjuude käigus kogutud info kasutajate hinnangutest oma oskustele tarkvara paigaldamise ja kasutamise osas, kogemustest viiruste ja rämpspostiga toimetulekul, teadmistest selle kohta, kes ja kuidas interneti ja arvutitega seotud probleeme lahendavad, usaldusest internetti oma andmete edastamise ja sealt saadavate andmete osas ning intervjuueeritavate suhtumine kommentaaridesse. Lisaks ka intervjuueeritavate võimalused arvutitega seotud probleemide kohta meediast infot saada.

4.1. Hinnangud oma oskustele

Intervjuueeritavatele esitati küsimus selle kohta, kuidas nad hindavad oma oskusi interneti- ja arvutikasutajatena võrreldes teiste kasutajatega.

Tabel 4.1

Hinnang Interneti ja arvuti kasutamise oskustele

	Oskaja	Keskmine	Nõrk	x
Naised	3	4	1	1
Mehed	1	3	1	1

Paigutades vastusevariandid tabelisse selgus, et suurem osa kasutajaid peavad enda oskusi keskmisteks või headeks. Näha on erinevust sooliselt – nimelt arvavad naised rohkem, et nende oskused on head. Tulp 'x' tähendab seda, et antud küsimustele vastates ei väljendanud intervjuueeritavad ennast selliselt, et neid oleks saanud vastuse põhjal mahutada ühte kolmest grupist. Küll võib aga öelda, et nad kuuluvad pigem gruppi „nõrk“. Peamiseks aluseks hinnangu andmisel on vastanutel kogemused kas üldise arvuti ja Interneti kasutuse või oma tööprogrammide osas. Seega kokkuvõtvalt viieteistkümnest inimesest üksteist peavad ennast keskmiseks või oskajaks kasutajaks.

Intervjuueeritavate käest uuriti kas neile meeldib ennast täiendada. Enesetäiendamist saab pidada oluliseks komponendiks riskiühiskonnas toimetulemisel. Ütleb ka ju Giddens (1999) : “Riskiühiskond on ühiskond, kus elame üha rohkem kõrgtehnoloogilisel piiril, mida mitte keegi enam täielikult ei mõista“, ehk selleks, et paremini toime tulla, peame

me pidevalt õppima. Õppimine ei muuda iseenesest veel mitte-spetsialiste spetsialistideks, küll aga aitab kaasa teadmiste lõhe vähendamisele nende kahe pooluse vahel.

Enesetäiendamise osas vastasid kõik intervjuueeritavad, et neile kas meeldib või nad tahavad ennast täiendada. Intervjuueeritavate käest küsiti täpsustuseks, kas koolituse jaoks on vajadust olnud isiklikel või tööalastel põhjustel.

Töökoha kaudu enesetäiendamine võib tulla nii inimese enese huvist või on koolituse algatajaks olnud töökoht. Näiteks vastati enesetäiendamiste kohta, mis on töökohaga seotud nii:

„Aga töö täiendused on kohustuslikud, igasugu asju peab tegema....“ (N1)

„Jaa, selle juhiasja koha peal kohe kindlasti. Eriti nüüd kohe, kui võetakse vastu uus asjaajamiskord, mis on mingi ISO, mingi asi Austraalia näitel ja ütleme, et kui ma hetkel töötaks, siis ma peaksin asutuses tegema kõik asjaajamisdokumendid ehk siis juba seesama asjaajamiskord, mis mulle meeldib, ära ... käskkirjad, protokollid, toimikute loetelud, arhiveerimise... noh, see tuleks kõik siis ümber teha. Kaasajastada. Aga kuna hetkel, hetkel nagu, hetkel ma ei tee midagi, siis ma nagu ei oska öelda, aga muidu põhimõtteliselt küll, seal oma töös ma ikka käisin tihtipeale, mitte tihtipeale, aga no ütleme, et aastas korra kindlasti mingil koolitusel. Et just selle töö alasel. Et viimane kord oli tööohutuse suhtes, et kui ma restoranid on nagu nad on, siis oli vaja seal materjalidega ringi käia ja lube anda ja kõik need seadused, mis on, vaja selgeks teha. Aga noh, meie seadused on ju rohkem kui kahtpidi mõistetavad, nii et mine võta kinni.“ (N5)

„Nii tööga oleks vaja kui isikliku eluga oleks vaja. Et see on mul plaanis. Et siis kui teine laps mul natuke suuremaks kasvab, siis on plaanis, jah“ (N6)

„...rohkem ikka vist tööst on johtunud need, tööga seoses ikka vist need täiendused enamasti olnud. Noh, küll arvuti, siis käsitöö suhtes ma käisin kursustel ja ikka, jah... praegu ma tahan ka minna ennast täiendama, aga see on ikkagi seotud jälle tööga“ (N8)

„Kui ma teeksin erialast tööd, siis ma peaksin kohe kindlasti täiendama. /.../ Keeleliselt peaksin... Vene keelt on vaja õudsalt palju“ (N9)

„valdavalt jah, valdavalt tööalased“ (M1)

„Elus ja töös on kindlasti vaja täiendust. Seda pidevalt ja kogu aeg“ (M4)

„Nojah, nüüd firma saadab seal kursustele. Sinna neid tehnikavärgid“ (M6)

Isiklikku laadi enesetäiendushuvide kohta vastati nii:

„Neid isiklike asju ikka ette tuleb ja need nagu meeldivad mulle rohkem“ (N1)

„kui keegi tuleks ütleks mulle, et ma saaksin hetkel tasuta suhtekorralduskursustele, siis ma juba jookseks“ (N5)

„Noh, kuna, kuna just see õppetöö, millega ma tegelema hakkas nüüd edaspidi, et see on selline natuke teistmoodi taustaga kui varem, siis selle tõttu on vaja ka, et nii palju lugeda ja... siis selle tõttu on ta huvitav ja niuke... et, et kui oleks võimalik, siis muudkui loeks, aga lihtsalt kogu vaba aega ei õnnestu selle peale kulutada“ (N7)

„mingid muud teadmised, mingid huvitavad faktid maailmast, mida võib-olla ei teadnud või oled ära unustanud kooliajast, lihtsalt selles mõttes, see on nüüd teatmeteosed“ (M1)

„Praegu mul näiteks seesama arvutiraamat siin laua peal, vaatan, kuidas jälle midagi teha ja siis ma vaatan, naine on toonud mul siin mingisuguse ajakirja, kuidas kodus ehitada (naerab), kuidas seal panna mingisugust põrandapuitu või asja, nii et no kogu aeg uurib, jah. Ei, meeldib küll jah. Ega ei saa ju olla tunnet, et nüüd ma kõike oskan. Nii et igalt poolt. Kui saab ja ikka võimalus on, siis panen kõrva taha ja võtan osa ja kuulan ja...“ (M3)

„muidugi on koolis ka hästi palju vaja neid asju, aga rohkem enda täiendamiseks nagu“ (M5)

On märgata erinevust, et kui tööalaselt käiakse enamasti koolitustel siis isiklike huvide osas loetakse rohkem raamatuid.

Arvutitega seotud koolitusi paraku ei mainitud, ainult üks intervjuueeritav mainis, et tal loeb arvutiga seotud raamatut. Nii huvi puudumine antud teemaga koolituste vastu kui ka vastavasisuliste koolitustega mittekokkupuutumine viib meid küsimuseni – mil moel saavad inimesed arvutialaseid teadmisi ning kogemusi?

4.1.1. Tarkvara paigaldamine ja kasutamine

Tarkvara paigaldamise, haldamise ning kasutamise oskus on tänases arvutimaailmas väga oluline. Erinevalt olukorrast kümmekond aastat tagasi, kus ostetud arvutit koos tarkvaraga kasutati nii nagu ta oli, on tänane situatsioon muutunud selliseks, et peaaegu iga päev tuleb kasutatavast tarkvarast välja uusi versioone. Uuendused seisnevad nii sisulistest uuendustes kui ka turvaparandustes. Kuna me elame Internetiajastul, kus Internetti ühendatud arvuti omab kokkupuudet kõigi teiste Internetti ühendatud arvutiga ning seega on kättesaadav kõigile ohtudele, siis on oluline, et kasutajatel oleks arvutis võimalikult uus ning turvalisim versioon antud programmidest. **Programmade mitteuuendamine suurendab riski sattuda küberohvriks.**

Intervjueeritavateelt küsiti koos hinnanguga oma oskustele ka hinnangut tarkvara osas - „*Kuivõrd oskajaks peate ennast vajaliku tarkvara leidmisel, installeerimisel, vajadusel eemaldamisel või kaasajastamisel?*“

On olemas kasutajad, kes pöörduvad esimeses järjekorras kohe spetsialisti poole, lastes probleemi lahendada ise sellesse süvenemata:

„*Ma pole seda teinud, ma lasen teistel teha.*“ (N2)

„*Ei, mis mul siin, mul ei ole... mina ei tea midagi.. ei... mul siin nooremad kõik, kes on teind, mina ei tea midagi.*“ (N4)

„*Ma kutsun kohe abi.*“ (N6)

„*Issand jumal! No neid ma ei oska üldse. Ma olen suutnud hakkama saada kunagi sellega, et olen installeerinud erinevaid keeli omale arvutisse, mida mul kindlasti vaja on. Printerit olen ka installeerinud. Programmid – ei*“ (N9)

„*Ei, seal ma ei tea üldse neid asju, ma ei oska üldse midagi teha. Sest kuna ma põhiliselt arvutiga tegelen koolis, siis meil on arvutispetsialist, kes Kui midagi on, siis ta kohe tuleb ja teeb ära*“ (M3)

On ka kasutajaid kes üritavad probleemiga tegeleda, ent neil puuduvad kogemused ning tulemuseks on mittesoovitud tagajärjed:

„*No installeerimisega... sellega ma vist oma arvuti tuksi keerasingi. Mina ei viitsi neid jutte lugeda, et kas on Yes või No. Et tavaliselt ma olen ikka Et tavaliselt ma*

olen ikka Yes pannud kogu aeg ja sellega ma vist keerasingi oma arvuti tuksi. Et ma ei jaga nendest programmidest ja asjadest eriti midagi. Kuna mu onu töötab arvutite ja nende asjadega ja on terve elu töötanud, siis tema tegeleb tavaliselt nende asjadega.“ (M4)

Kasutajad kes lahendavad tarkvaraga seotud probleemid ise, võib jaotada kaheks: esimesed on valdkonnast täiesti teadlikud ning teavad mida on vaja teha ja teised, kes saavad tarkvara haldamisega hakkama etteantud juhiste järgi:

„Noh, kui juhend on olemas, siis saab ikkagi hakkama, ütleme, et selles suhtes nagu probleemi ei teki.“ (N3)

„Ma arvan, et no ütleme siis nii, et ämmal sai plank arvuti ostetud ja kõik asjad panin mina sinna peale. Nii et kui on plaat ees ja arvuti minuga suhelda oskab inglise keeles ja mina temast aru saan, siis ei ole ju probleemi.“ (N5)

„Mmm, kui see on hästi mugavaks tehtud nagu Windowsil kipub olema, et vajutad lihtsalt, et ta otsib sulle mingisuguse uuenduse ise välja ja siis sa pead vajutama ainult nuppudele, siis loomulikult saab hakkama, aga, aga ma olen ise otsinud ka neid... enamasti mingeid siukseid vabavara asju, mida saab kergesti kätte ja neid üldiselt on ka väga lihtne peale panna.“ (N7)

„Ma arvan, et ma saan sellega hakkama, aga... tähendab ma arvan, siiani olen saanud“ (M1)

„See on siia maani ka nagu sujund kõik.“ (M2)

„no nüüd ei ole mingit probleemi, on nii palju lehekülgi, kust saab tarkvara alla tõmmata endale ja paigaldada ning eemaldamisega pole ka mingit probleemi.“ (M5)

4.1.2. Kogemused viiruste ja rämpspostiga

Uurisime kas intervjuueeritavatel on kogemusi viiruste ja rämpspostiga ning kas nad oskavad midagi nende vastu ette võtta. Küsisime „On teil olnud kogemusi viiruste, rämpsposti vms. ebameeldivustega?“

Viiruste kohta vastas enamus, et neil on olnud selle probleemiga kogemusi:

Jah, on küll olnud. Seda on küll olnud, et siin on igasugused asjad olnud, et linnukesed lendavad või värgid ja... jah, jah... on näha küll, et on rämpsud olnud ja.. aga mina ei tea, mina ei ole seda näiteks teinud, aga ka mul jälle pks noorem on olnud siin, siis on teinud seda puhastust jälle või resetti, mina ei tea, kuidas nad seda teevad või... et kustutab kõik ära ja.. aga mina ei ole teind seda!(N4)

Ja veel kuidas! Viirustega minu arust pool arvutit, Kaspersky minu arust ainult karjus. Ja seal tuli ikka nii konkreetne viirus sisse, et oli kohe tulnud, et ikka itimehel läks sellega ikka tükk aega, enne kui ta selle sealt arvutist kätte sai. Aga õnneks teised arvutid olid võrgus küll ühendatud, aga need õnneks ei saanud seda viirust. See oli mingi ussviirus, ma mäletan veel, paar aastat tagasi, see oli ikka jube.(N5)

Jah, on küll. Ja iga päev. (N9)

Jah, kui nagu midagi sinna tuleb või... ma tean, et on ju kaitstud, eks, on ju programmid (M1)

On küll, kusjuures viimasel ajal järjest tihedamini, nad ikkagi levivad päris ohtralt (M2)

Rämpsostiga oli samuti kokkupuude enamusel olemas, mitmel korral selgitatakse, et rämpsostu vastu üritatakse võidelda erinevate võtetega, kasutades filtreid ning ajades tööasju töömeili pealt, nii et sõprade jaoks on eraldi meiliaadress:

Iga päev. /.../ Tähendab, kasutan küll. Noh, mul on isiklik meil ja töö meil, eksju. Ja-ja.. mul on kolm meili. Noh, on nagu ikkagi mingi vahe, et kui sa pead kellelegi selle meiliaadressi andma, siis sa mõtled, et kui tihedalt mul on temaga vaja suhelda, et kas ma annan talle igapäevase meili või selle meili, mille postkasti ma ära kasutan. Et las läheb sinna, mida ma vaatan üks kord kuus või üks kord nädalas, mida ma vaatan ja siis lihtsalt kustutan. (N1)

No oma hotmaili ma olen ära protectinud nii, et need meiliaadressid, mis mul on endal kontaktide all, need tulevad inboxi ja need mida mul ei ole need lähevad kohe automaatselt junk maili ja junk maili alt ma vaatan, kas on mõni tähtis asi mis peaks mulle silma jääma. Nii ma olen nagu teinud. Ja kodus on mul arvutil on

loomulikult ka viiruskaitse, tõrje, et teistmoodi ei saagi. (N5)

Jaaa, rämpsostile ma panin lihtsalt peale filtri, et ta sorteeriks välja, mis vähegi kahtlased tunduvad. Et sellega seoses on küll niimoodi, et ta paneb aeg-ajalt asjalikke kirju ka sinna hulka, et siis tuleb need välja nokkida, aga et toimib hästi.

Ja viirusetõrjet ma nagu ka kasutan. Noh, on vaja ise uuendada, et ta... (N7)

Ikka erinevad on, jah, Noh, neid on nagu kolm... /.../ Töö oma, sõbra oma... (M1)

Need on nagu üksteisest lahus (M2)

On aga ka neid, kes ei oska kasutada e-maili filtreid või võtta kasutusele muid meetmeid:

Selles mõttes jah, jaa, ei, kahtlaseid asju kustutan kohe ära, seda ma oskan jah. Aga noh, see, et viirusetõrjet ei oska peale panna ja noh, ühesõnaga... Kogu aeg öeldakse, et pane omale filter vahele, et tuleb jube palju rämpsposti, et pane filter vahele, et näed see on nii lihtne sealt kohast, ma ei ole vaadanud. Aga kustutada ära ma oskan küll (N2)

Ei oska. Nojah, ei ma muud ei tea ja ma vaatan seda rämpsust ja mis ei kõlba, selle kustutan kohe ära (M3)

Ma tean, et on olemas tulemüür ja siuksed asjad, aga ma ei tea, kust neid saab ja kes neid saab, ma ütlesin onule, et pangu mulle siis kõik need süsteemid (M4)

Kokkuvõttes võib öelda, et hinnangutes oma oskustele viiruste ja rämpsostiga võitlemiseks pidasid ligi pooled intervjuueritavatest oma taset keskmiseks ning umbes veerand nõrgaks. Arvestades nende jutust esile tulnud oskustega võib öelda, et iseseisvalt need inimesed kõigi sellist laadi arvutiprobleemidega, mida saaks teadliku käitumisega vältida, toime ei tule. Positiivseks tuleb pidada seda, et kõik on huvitatud üldisest enesetäiendamisest ning kogemuste juurde saamisest, küll aga ei maininud keegi, et täiendust oleks vaja arvuti vallas. Seda kinnitas ka küsimus viiruste ja rämpsikirjade kohta kus intervjuueritud ütlesid, et neil on kogemus nende probleemidega, ent samas paljud ei osanud võtta kasutusele konkreetseid vastumeetmeid nende vastu.

4.2. Probleemide lahendamine

Vastajatel paluti selgitada, kuidas lahendatakse arvutite ja Internetiga seotud probleemid. Ei uuritud konkreetselt seda, kas probleemide lahendamine kodus ja tööl kuidagi erineb, kuid sellegipoolest joonistus välja, et tööl ning kodus käituvad inimesed arvuti ja Internetiga seotud probleemide lahendamisel erinevalt.

4.2.1. Kes lahendavad probleeme

Arvutite ning Internetiga seotud probleemide lahendamises leiab intervjuudest üsnagi erinevaid variante, millest põhilised on järgmised:

- Probleemid lahendab arvutikasutaja ise
Kui vooluvõrgust välja lülitab, siis ma oskan ise ära parandada. Aga oleneb probleemist. (N1)
Igäüks vastutab oma arvuti eest ise (N3)
- Probleemid lahendab keegi perekonnast
Siis otsib poeg edasi, minul on ainult esimene asi... (N2)
Oma noored lapsed, poeg. (N4)
- Probleeme lahendavad sõbrad
Kui ta pildi taskusse viskab, siis ma võtan ta kaenlasse ja lähen oma sõbra juurde (N5)
Ei, asjatundjate poole ma ei ole pöördunud, sõprade poole. Nendest on abi, see on hea. (M5)
- Probleeme lahendavad töökaaslased
Jah, nii palju kui oskan. (M2)
Olen juhendanud. Aga noh, see on selline... Kah pigem see on selline lihtsalt endale teada, mida ... nikerdada, et kuidas mingit programmi kasutada või midagi sellist. (N7)
- Probleeme lahendab töö juures olev arvutispetsialist
[pöördun] /.../ selle vastava osakonna poole. (N6)
Asjatundjate poole. (M4)

Paljude firmade arvutipoliitika on liikunud sellisele tasandile kus tavakasutaja ei saagi enam ise midagi teha – piiratud on kõik õigused teha süsteemseid muudatusi ning iga väiksemagi probleemi korral on kohustus pöörduda vastava osakonna või töötaja poole.

Grupi „probleemid lahendab arvutikasutaja ise“ juurde tuleb öelda selgituseks veel niipalju, et ise püütakse lahendada kergemaid probleeme ning keerulisemaid vähesel määral – kui triviaalne lahendus ei aita, siis pöördutakse juba teiste võimaluste poole, kasutades sõprade, tuttavate või arvutispetsialisti abi.

4.2.2. Juhendatavad muutuvad juhendajateks

Huvitav on näha muutust juhendamises seoses keskkonna muutumisega. Enamus vastanuid vastasid küsimusele „*Kas ise aitate või juhendate teisi arvuti kasutamisel?*“ jaatavalt. Uurimisel selgus, et juhendatakse neid, kelle teadmised on veel väiksemad ning seda tehakse enamasti olukorras, kus ei ole suuremate teadmistega inimest. See tähendab, et näiteks tööl olles võib inimene olla juhendatav samas kui kodus muututakse juhendajateks või vastupidi. (K – küsija ehk intervjuuerija, V – vastaja ehk intervjuueeritav)

K: Kas ise aitate või juhendate teisi arvuti kasutamisel?

V: Jaah.

K: See on siis nagu kodus?

V: Ei, pigem töö juures.

K: Aga kodus teil on arvuti olemas?

V: Jah.

K: Ja seal lahendab enamasti selle probleemi...?

V: Arvutispets.

(N1)

K: Kas te ise aitate või juhendate teisi arvuti kasutamisel?

V: Jah, on ikka tulnud ette küll.

K: Kui teil on kodus arvuti, kes siis enamasti lahendab arvuti hooldamisega seotud küsimusi?

V: Poeg.

(N2)

K: Aga aitate või juhendate teisi ise ka arvuti kasutamisel?

V: Olen juhendanud. Aga noh, see on selline... Kah pigem see on selline lihtsalt endale teada, mida ... nikerdada, et kuidas mingit programmi kasutada või midagi sellist.

K: Kui teil kodus on arvuti, siis kes teil enamasti lahendab arvuti hooldamisega seotud küsimusi?

V: Mmm... antud juhul abikaasa. Et temal on, temal on... võimalus rohkem ringi käia selle arvutiga

(N7)

K: Kas sa ise oled ka juhendanud või aidanud teisi arvutite kasutamisel?

V: Jaa, natuke olen. Üks sõber mul hakkas alles hiljuti arvutit kasutama, teda ma natuke õpetan. Aga noh, see on seal niivõrd väike osa.

K: Kui sul on kodus arvuti, siis kes enamasti lahendab arvuti hooldamisega seotud küsimusi?

V: Onu lahendab. Või siis noorem vend, kes seda asja natuke rohkem jagab, tema on ka seal vaadanud.

(M4)

4.2.3. Lahenduste mudelid

Intervjuudest saadud andmete põhjal saab esmase probleemide lahendamise järgi joonistada välja järgmised grupid:

1. Kasutaja lahendab probleemid nii tööl kui kodus (N1, N5, M2, M6)
2. Kasutaja lahendab probleemid kodus ja tööl teeb seda keegi teine (N3, N6, M1)
või kasutaja lahendab probleemid tööl ning kodus teeb seda keegi teine (N2, N7)
3. Kasutaja ei tegele ise üldse probleemide lahendamisega (N4, N8, N9, M3, M4, M5)

Arvutite ja internetiga seotud probleemidega on kõige rohkem kursis esimese grupi esindajad, püüdes probleemidega ise kõigepealt hakkama saada. Spetsialisti poole pöörduakse siis kui ise enam hakkama ei saada :

„Kodus on, enamuse asjadega saan hakkama. Ütleme nii, et ma olen selles olukorras, kus ma tahaks osata rohkem. Ma ei jää hätta. Ma ei jää hätta töö juures, ma saan kodus hakkama“ (N1)

„Kui ta pildi taskusse viskab, siis ma võtan ta kaenlasse ja lähen oma sõbra juurde, aga muidu, ma ei tea, noh... Vahest ta jookseb kokku ja vahest ta tahab, et talle disk cleanupi tehtaks. /.../ sellega ma saan hakkama“, „Mina, lahendan mõlema arvuti probleeme (kodus)“, „Ja hooldusega? Täpselt samamoodi mina“ (N5)

„enamuse asjadega saab nagu hakkama, aga mingi nii-nimetatud häkker ma nüüd ei ole“ (M2)

„Siia maani olen ise hakkama saanud. Nii palju oskad ise ja kui ei saa, siis spetsialisti poole“ ning küsimusele „Kui sul on kodus arvuti, siis kes enamasti lahendab arvuti hooldamisega seotud küsimusi?“ vastas „Mina, mina olen teinud“ (M6)

Teise grupi juures võib täheldada, et inimesel on olemas teadmised probleemide lahendamiseks, aga kas tööl või kodus on olemas keegi kes oskab arvutite probleeme paremini lahendada ning seega delegeeritakse ka probleemide lahendamine edasi:

K: Kui teil on kodus arvuti, kes siis enamasti lahendab arvuti hooldamisega seotud küsimusi?

V: Poeg.

K: Kust te veel leiate abi probleemide lahendamisel?

V: mismoodi?

K: Kui näiteks poeg ka hakkama ei saa, mis te siis, kas te otsite kusagilt või?

V: Siis otsib poeg edasi, minul on ainult esimene asi...

(N2)

K: Kui teie arvuti töös tuleb ette tõrkeid, kas oskate neid ise lahendada või pöördute asjatundjate poole?

V: See oleneb tõrkest, et standard lahendused, need teab ikka ise ära ja saab järgi proovida, et... /.../ noh, nendest saab üle, ütleme niimoodi. Kui tekib mingi selline, mingi hull seis, et noh, arvutil mingi asi saab vanaks, läheb katki, siis enam nagu

ei saa... /.../

K: Aga mis tüüpi probleemidega on teil arvutiga seoses enamasti tegu olnud?

V: Noh, põhiprobleem on see, et see Internetiühendus on aeglane või kaob üldse ära, et see on. Ja, ja, ja aeg-ajalt on on Windowsi süsteem... nii-öelda kukub kokku, et ta ei hakka enam... lõpetab üldse suhtlemise ära, et see on nagu programm. Ütleme, et need on nagu kaks sellist suuremat, sagedasemat.

K: Aga kui teil on kodus arvuti, siis kes enamasti lahendab arvuti hooldamisega seotud küsimusi?

V: Igaüks vastutab oma arvuti eest ise. Meil on kodus selline lugu, et oma arvuti eest hoolitsen mina ja isa hoolitseb oma arvuti eest ise ja kui meil mõlemal juhtmed kokku jooksevad, siis tuleb vend appi.

(N3)

Kolmandasse gruppi kuulujaid saaks iseloomustada modernsele ühiskonnale omase suhtumisega – probleeme peavad lahendama spetsialistid. Kindlasti aitab ka spetsialistide olemasolu kaasa probleemide lahendamise edasidelegeerimisele ning probleemide lahendamiseks vajalike teadmiste ja kogemuste mitteomamine. Samuti võib olla selline käitumine seotud firmasisesse IT-poliitikaga kus peale arvutispetsialistide ei tohi ega saagi keegi teine midagi teha.

K: Kui teie arvuti töös tuleb ette tõrkeid, kas oskate neid ise lahendada või pöördute kellegi poole?

V: Pöördun.

K: Kelle poole?

V: No selle vastava osakonna poole.

K: Kui teil on kodus arvuti, siis kes enamasti lahendab arvuti hooldamisega seotud küsimusi?

V: Mees. Või siis küsin jälle endal töö juurest abi.

(N6)

Probleemide lahendamisega tegelevad ise vähesed, enamasti pöörduakse ikka kas teiste perekonnaliikmete, sõprade või töökaaslaste poole. Samas ilmneb tõsiasi, et inimesed, kes tööl või kodus olles küsivad teistelt abi osutuvad samas teises olukorras juhendajateks.

Kuivõrd adekvaatne õpetus sellisel moel edasi antakse antud töö ei uurinud, kuid seda võiks kindlasti edasi uurida mõne teise töö raames. Juhendamisega sarnaselt tuli välja ka lahenduse mudelid, kus kasutaja võis lahendada kõik probleemid alati ise, või siis lahendas ainult kas kodus või tööl jättes mujal probleemid teiste hoolde.

4.3. Usaldus

4.3.1. Isiklike andmete edastamine Internetti

Isiklike andmete edastamine Internetti võib toimuda kahel moel – teadlikult ja mitteteadlikult. Teadliku edastamisena saab käsitleda sellist olukorda kus arvutikasutajal palutakse edastada kas veebilehe, maili või mingi muu kanali kaudu oma isiklikke andmeid, koode, telefonide numbreid jne. Mitteteadlik andmete edastamine toimub enamasti arvutikasutajale märkamatuks – arvutisse on lisatud nuhkvara programm mis jälgib arvutikasutaja teadmata kõiki tema tegevusi ning edastab saadud informatsiooni Interneti. Nende kahe võimaluse vahele mahub ka veel andmete väljapetmine, kus inimene petetakse ära tuntud teenusele sarnase veebilehe või mailiga ning palutakse edastada andmeid (näiteks panga kujundusega leht, kus palutakse sisestada oma PIN koodid).

Uurisime kas inimesed annaksid ise andmeid Internetti. Näiteks on osad inimesed nõus oma andmeid valikuliselt Internetti edastama, aga seda juhul kui teine pool on usaldatav – näiteks pangale:

K: Kas te annaksite Internetti oma isiklikke andmeid?

V: Väga-väga valitult (mõttlikult).

K: Millega seoses see võiks olla, et kas näiteks mingi panga, Internetipanga...?

V: See on jah just täpselt, et kui oled Internetipangas, et seal teha, siis paratamatult teatud aspektid ja ütleme Internetipoodides, see on ju paratamatult ka, et annad mingi informatsiooni, aga... aga ülejäänud puhkudel ütleme minimaalselt vähe, ütleme selles mõttes. Ja kui liiga palju küsitakse, siis ma loobun kasutamisest.

(N3)

Osad intervjuueeritavad ei olnud üldse nõus oma andmeid edastama

K: Kas te annaksite oma isiklike andmeid...

V: Ei-ei-ei-ei, mitte iialgi! Ma saaks kohe aru, et see... ma, ma ei usalda. Ma iialgi ei usaldaks.

(N4)

K: Aga kusagile näiteks oma krediitkaardi numbrit näiteks?

V: Ei, ei! Kindlasti mitte, kindlasti mitte.. See peab päris rumal inimene olema, kes seda teeb

(M1)

Ning mitte-edastamist põhjendati ka sellega, et selleks pole lihtsalt põhjust

V: Mul pole krediitkaarti, nii et pole probleemi.

K: Aga kas te annaksite Internetti oma isiklike andmeid?

V: Mkm. Ei, mis ma neist ikka siia ülesse panen, kellel neid vaja on. Mina tean, kes ma olen ja need teavad ka, kelle vaja teada on ja need, kes ei tea, järelikult need on sellised institutsioonid, kes tahavad kohe minna ja teada seda.

(N5)

4.3.2. Internetis leiduva info usaldamine ning kasutamine

Intervjuueeritavate käest küsiti kas nad usaldavad Interneti vahendusel toimuvat suhtlemist. Leidus nii selliseid kes vastasid positiivselt

„Tegelikult ma arvan, et ma usaldan.“ (N1)

„No ma vist ikka vist usaldan. Ei ole tekkinud mõtet, et kas ma nüüd usun või ei usu.“ (N6)

„Mm, jah. Ma olen küll suhelnud väga toredate inimestega“ (N8)

„No 99 % ikka.“ (M6)

kui ka neid kes olid pigem mitteusaldavad

„Ega ma ei usaldaks küll, kui ma noh, niiviisi... See on ikka väga hea valetamise koht. Et noh, näiteks see, et ma nüüd tutvusin kellegagi Internetis ja usuksin,

mida ta seal kirja paneb, seda ei ole. Ühesõnaga ma väga kahtleksin selles, mis on... muidugi on võimalik, et tõesti inimene on aus, aga noh, see paistab pärast“ (N2)

„Eriti ei usalda, aga samas ma ei lähe ka sinna sellisel eesmärgil, et hakkaks kedagi usaldama“ (N9)

„Ei, sada protsenti kindlasti mitte, ega peab ikka jälgima, mida üles panna, mite mitte, kuidas ta kaitstud on, noh, kõik need asjad.“ (M1)

„Ma arvan, et seal tuleb nagu endale selgeks teha ja aru saada, et kes räägib õiget juttu ja kes räägib mingit jama“ (M2)

Samas kohtab vastuolu – näiteks inimene kes usaldab Internetisuhtlust ei usalda siiski Internetist tulevat infot:

K: Kui te kusagilt foorumist, ajalehest saate mingisuguse info, eluaseme, töö, tervise kohta, siis kas te kontrollite seda infot?

V: Ei

K: Usaldate seda?

V: Ei usalda. Seda infot ma küll ei võta. Kommentaariinfot.

(N1)

Üldiselt ikkagi arvatakse, et Internetist tulevat infot on vaja kontrollida kui just info ei tule ametlikest kanalitest.

Noh, oleneb olukorrast ja oleneb infost täiesti. Kui on Internetis korralik info saadaval, siis kontrollin sealt üle või kui on tutvusringkonnas mõni sihuke spetsialist, siis uurin sealt järgi (M2)

Ei tea, noh... Ega ma väga ei usalda, aga noh... (naerab) Mõtleb, võtab mõtlema või niimoodi arutama või... Siis tuleb ikka läbi seedida ja vaadata, mis seal siis nüüd on või... Noh, te küsite, mis asi see võiks olla, mida ma seal... Noh, ma ei tea. No kui mingi näiteks antakse edasi mingisugust valitsuse määrust või mingit seadust, no siis ma ikka usun seda (M3)

Eem, kriitiline meel peab alati olema. Selles mõttes, et kui see tundub nagu loogiline, siis ütleme ta jääb nagu positiivse info hulka. Aga noh, ma alati üritan võimalikult palju teada saada igast asjast, enne kui ma mingi otsuse teen minu jaoks võõral temaatikal. Nii et ütleme, absoluutselt ma ei usalda, seda kindlasti

mitte. (N3)

Ei, niimoodi ma ei hakka uskuma, iial ei või teada ju, mis sinna üles pannakse. Kui ta on juba noh, ütleme, et kui ta on juba Päevalehest läbi käinud ja Äripäevast läbi käinud, no siis juba tasub uskuda (N5)

Oleneb, mis info see on. Kus on need portaalid, kus need inimesed seal sõna võtavad, neid ju ei usalda. /.../ Sellepärast, et seal ju võib igasuguseid asju kirjutada. Aga kui on midagi siukest ikka noh näiteks keerulisemat, neid ikka usaldan. (N6)

Noh, niivõrd kuivõrd, eks teda tuleb ikka seedida ja mõelda ja vaadata ja arutada. (N8)

Seoses kontrollimisega esineb arvutikasutajatel probleem, et täpselt ei osata öelda kuidas peaks infot kontrollima

No tähendab, ma olen, kuidas ma nüüd ütlen, saanud ebausaldusväärset informatsiooni, aga kontrollisin siis oma naha peal. Näiteks bussiajad on internetis valed olnud. Siis on see, et ma olen tööga seoses neid Internetiaadresse või e-maili aadresse võtnud, mis on valed. Nii et elu on öelnud, et ära usu. Aga tähendab, üle ma ei kontrolli küll, kui ma olen infi saanud, siis ma võtan selle kasutusele ja eks elame näeme. Aga ma ei tea, kuidas ma peaks üle kontrollima (N2)

4.3.3. Suhtumine kommentaaridesse

Peaaegu kõik uudisteportaalid pakuvad lugejatele võimalust ka uudiseid kommenteerida, avaldada teema või uudise kohta oma arvamust kohta ning edastada omi kogemusi. Intervjueeritavate käest küsiti, kuivõrd need kommentaarid peegeldavad avalikku arvamust selleks, et seeläbi vaadata nende üldist suhtumist anonüümselt edastatud informatsiooni. Kommentaaridesse suhtumise ning usalduse küsimus on oluline selgitamaks, kas inimesed on üldse valmis omastama informatsiooni, mis Internetist tuleb kommentaaride näol.

Valdavalt arvatakse, et kommentaarid kas peegeldavad väga väikese grupi inimeste arvamust, või siis negatiivset arvamust.

„Nad peegeldavad negatiivset arvamust .. on pigem selle negatiivse poole arvamus.“ (N1)

„Nad peegeldavad ütleme sellist agressiivset arvamust.“ (N3)

„Oleks väga kahju tegelikult, kui peegeldaks. Ma ei usu, et need inimesed, kes seal kirjutavad, tegelikult niimoodi mõtlevad, selle pärast, et nad tahavad lihtsalt vahvad välja paista. Või ma ei tea. Kui neid nagu kanda üle selle põhjal üldine arvamus, siis selle põhjal on väga palju rumalaid inimesi, kes julgevad seda välja näidata.“ (N9)

„No mingil määral seal Interneti teel paljud nagu ütlevad välja, mis nad tegelikult mõtlevad, anonüümselt... Aga ma ei ütleks küll, e ta täiesti üldsuse arvamust...“ (M2)

Samuti arvati, et kommentaarides väljendatud arvamused on võimendatud kujul või siis väljendatud julgemalt

„Ta on avaliku arvamuse, ütleme, suurendusklaas. Et kui avalik arvamus üldiselt suhtub negatiivselt, siis ikka seal, noh, on kohe hirmus pahasti öeldud.“ (N2)

„Internetis on inimesed julgemad, siis nad kirjutavad seal kõike, mida nad tahavad, aga üldiselt avalikus elus ikka ei öelda niiviisi, ainult Internetis. Aga ma ei oska nii öelda, sest ma ei loe neid ja ma ei tea, mis nad sinna kirjutavad. Aga ma arvan, et inimene on Internetis julgem ja saab anonüümseks jääda, keegi niikuinii teda ei näe.“ (M5)

Suhtutakse umbusklikult ent samas tõdetakse, et kommentaaride seas leidub ka asjalikke arvamusi.

„Eks ta mingil määral peegeldab, aga see ongi nagu ainuke asi, mida ei taha usaldada, ta on seal avalik, sinna kirjutatakse mida iganes. Et ma loen neid, aga ega ma... vat need... kõvast välja teha, eriti need... tõsiselt küll ei võta neid kommentaare. Aga mõni on päris huvitav. Ma leian, et mingi protsent on kindlasti on selline, noh, mida saab nagu usaldada, aga neid on nii erinevaid, eks ta mingi protsent on kidnasti, mis peegeldab inimeste arvamusi.“ (N6)

„Mmm... kohati hästi, kohati mitte, sest just need lehekommentaarid on sellised, et

noh, läheb aeg-ajalt selliseks kirjutajate üksteisevaheliseks sõimamiseks ja sopaloopimiseks, et noh, see on jabur. Aga, aga on ka asjalikke kommentaare ja minu meelest... Siis ikka näeb nagu paremini, mida inimesed mingisugustest probleemidest arvavad ja mõtlevad, et see, mida linnaisad seal pealinnas arvata võivad või arvavad, et inimesed arvavad, et nagu see, see tihti seal ei ole nagu ikka seesama.“ (N7)

Intervjueeritavate seas oli ka neid, kes lihtsalt arvasid, et kommentaarid peegeldavad avalikku arvamust.

„No kindlasti peegeldavad, kindlasti peegeldavad seda inimeste arvamust. Arvamusi on ju palju ja, ja, ja noh, kui seda välja pelda, siis saabki teada, mida inimesed mõtlevad“ (N8)

Hinnangutes kommentaaridesse saame teha oletuse üldisesse suhtumisse nende sisusse. Võib öelda, et kommentaaridest leiduva info põhjal otseselt tegutsema ei hakata, hoolimata sellest, et seal võib olla adekvaatne info.

Usaldust isiklike otsuste suhtes antud töö ei uurinud, küll aga uuris kuidas usaldatakse Interneti info allikana ning kuivõrd ollakse valmis oma personaalseid andmeid Interneti andma. Isiklike andmete osas oli valdav enamus intervjueeritavaid kindlad, et niisama ei tohiks oma andmeid Internetti edastada, erandiks on ehk väga kindlad juhtumid nagu pank või maksuamet. Internetist tulevasse infosse suhtutakse üldiselt kahtlevalt ning peetakse oluliseks enne selle kasutamist seda kontrollida kas teistest allikatest või täpsustada sõprade-tuttavate käest. Sellest tulenevalt võib oletada, et Internetis arvutiturvalisuse kohta kirjutades peab see olema üsnagi tunnustatud leheküljel.

4.4. Info hankimine meediast arvutitega seotud probleemide kohta

Intervjueeritavate käest uuriti, kuivõrd pööratakse tähelepanu meedias ilmuvatele artiklitele. Täiendavalt sellele küsimusele uuris töö autor läbi intervjuude ajal ilmunud kaks päevalehte – Postimees ja Eesti Päevaleht perioodil 1.jaanuar kuni 28.veebruar. Selle aja sees ilmus nendes lehtedes 41 tehnoloogiaga (arvutid, Internet, robotid,

mobiiltelefonid) seotud artiklit. Neist ainult kaks artiklit oli seotud andmete lekkega ning üks uudis rääkis lühidalt rämpsposti vastasele võitlusele kulutatavatest summadest. Kaks artiklit oli olulised õiguslikust küljest rääkides failide jagamisega seotud seaduserikkumistest. Lähemalt vt Lisa 3.

Intervjueeritavad võiks jagada ajalehtedes ilmuvate artiklite lugemise järgi sellistesse gruppidesse:

1. Üldse ei loe artikleid.

K: Kas te ajakirjandusest jälgite kirjutisi, mis on seotud arvutiprobleemidega?

V: Tegelikult ei jälgi

K: Kas te arvutite ja Interneti kajastamist jälgite meedias?

V: Ei

(N1)

K: Aga kuivõrd te jälgite arvutiprobleemidega seonduvat näiteks ajakirjanduses

V: Ei, üldse mitte. Ja see, mis telekas on, see Arvutiaabits, seda ma ka ei vaata

K: Aga kui te näete arvutitega seotud lugu näiteks Päevalehes, kas te vaatate seda või liigute edasi?

V: No ma vaatan, mis see on, aga see pole kindel, et ma teda loen. Aga üldiselt, tõenäoliselt ei loe.

(N2)

K: Kui näiteks näete arvutitega seotud lugusid päevalehtedes, kas vaatate neid või liigute edasi?

V: Ei, ma ei vaata

(N4)

K: Kuivõrd jälgite arvuti probleemidega seotut ajakirjandusest?

V: Ei, üldse ei jälgi

K: Kui näiteks näete arvutitega seotud lugusid päevalehtedes, kas vaatate neid või..

V: Ei! Ei.

(N6)

K: Kui sa näiteks ajalehti loed ja näed seal mingeid arvutitega seotud teemasid, kas sa loed neid või lähed pigem järgmiste teemade juurde?

V: Lähem pigem järgmiste teemade juurde.

(M5)

2. Loeb väga harva, enamasti kui aega või kui on huvitav pealkiri. Loetakse enamasti kiiresti üle libisedes ning süvenemata.

K: Kuivõrd jälgite arvuti probleemidega seotut ajakirjandusest?

V: Ee, no selles suhtes küll, et need uudised jooksevad läbi, kui midagi on... enne teavitatakse, kui mingisugused probleemid hakkavad massiliselt levima või mingid viirused, et noh, selles mõttes. Ma spetsiaalselt otsima ei hakka, aga kui ma näen kuskil pealkirjas mingit viidet sellele, siis ma kindlasti vaatan.

K: Kui näiteks arvutitega seotud lugisid päevalehtedes, kas vaatate neid või liigute edasi?

V: Ee, see oleneb nagu temaatikast ja sellest kui palju mul on konkreetset aega. Kui on tavaline kiire päev /.../ siis ma sellele ei pööra tähelepanu. Aga kui on, noh, nagu natuke rohkem aega, töö seljas ei istu ja mõni aspekt on huvitav mingite rakendusvaldkondade suhtes, et kuhu edasi liigutakse ja midagi välja mõeldakse uusi asju, siis ma vaatan üle

(N3)

K: Kuivõrd jälgite te arvuti probleemidega seotut ajakirjanduses?

V: Ei jälgi.

K: Kui te näete arvutitega seotud lugusid näiteks päevalehes, kas te siis vaatate neid või liigute edasi?

V: Kui mingi hõkerdamine on, siis ma vaatan, aga kui keegi kuskile mingit võimsust juurde pannud on või graafikakaarti arendanud, siis ma ei oska seda hinnata. Et ma nagu jah neid asju ei oska nii hinnata.

(N5)

K: Aga olete tähele pannud, et Postimehes ja Päevalehes teinekord ilmub arvutiga seotud artikleid?

V: Jah, ma ütlen, kuskil ma olen näinud, aga nii täpselt ma ei oska...

K: Aga lugema ei ole neid hakanud või olete?

V: Tähendab, Ekspressis olen ikka vist midagi lugenud, aga oleneb ka sellest tasemest, ma arvan, et ikkagi...

K: Kui pealkiri tuttav ei ole, siis..

V: Jah, jah, siis ma neid lugema ei hakka. Kuna ma tõesti selle tark- ja

riistvaraga ei tegele, siis..

(N8)

K: Kuivõrd sa jälgid arvutiprobleemidega seotud ajakirjandust?

V: Ei jälgi üldse peaaegu. Mõnikord Äripäevas, kui on mõned artiklid võibolla Bill Gates'i kohta. Aga konkreetselt küll mitte.

(N9)

K: Kas sa seda oled tähele pannud, et näiteks Postimehes, Päevalehes aeg-ajalt kirjutatakse arvutite teemal?

V: Jah.

K: Sinna oled pilgu peale visand?

V: Reeglina ma loen nagu kõik pealkirjad... pealkirjad läbi, aga kui on nagu huvitav, mis kutsub lugema, siis loen ka sisu läbi.

(M2)

3. Loeb artikleid.

K: Kas jälgite ajakirjandusest arvutiprobleemidega seotud uudiseid?

V: Mmm, jälgin ikka, aga alati ei ole see nagu, noh, vajalikuks osutunud, selles mõttes on hästi läinud. Kasvõi see, et mingid hullud viirusepuhangud on liikvel, siis jälle lehest lugesin... Aga nüüd on telekast arvutiaabitsa sade, seda ma olen aeg-ajalt katsunud vaadata. Olen jälle üht koma teist huvitavat teada saanud, et mismoodi need masinad arenenud on ja neid uuendusi teada saanud.

(N7)

K: Kui näete näiteks arvutitega seotud lugusid päevalehtedes, kas siis nagu vaatate neid või liigute edasi?

V: Ei, ma ikka vaatan neid, jah.

(M3)

Intervjueeritavad mainisid lisaks Postimehele ja Eesti Päevalehele arvutialaste artiklite allikatena veel Äripäeva, Arvutimaailma ning Eesti Ekspressi. Samuti mainiti ära Kuku-raadios eetris olev saade Tehnokratt.

Riskiteooria järgi, kus riskiga seoses on väga olulisel kohal teadlikkus, peaksid inimesed igal võimalikul juhul püüdma saada juurde uusi teadmisi nende tegemistega seotud objektide kohta. Intervjuudest tuleb kohati aga välja vastuolu riskiteadliku käitumisega kuna meediast hangivad arvutitega seotud teemade kohta infot vähesed.

Järeldused ja diskussioon

Käesoleva töö fookuses oli arvutikasutajate käitumine seoses arvutitest ning Internetist tulenevate ohtudega ning nende ohtude seostamine riskiühiskonnaga. Ohtudest pöörati rohkem tähelepanu rämps kirjadele, viirustele ning isiklike andmete turvalisusele.

Andmeid koguti inimeste hinnangute, teadmiste ja arvamuste kohta arvutite ja internetiga seotud ohtudest ja nendega toimetulekust. Kasutati intervjuu-meetodit, kusjuures intervjuude valimisse kuulusid inimesed, kes olid osalenud Tartu Ülikooli Ajakirjanduse ja kommunikatsiooni osakonna 2002. aasta uuringus “Mina.Maailm.Meedia.” ning kes olid andnud nõusoleku edaspidistes uuringutes osalemiseks.

Kasutatud metoodika kohta võib öelda, et intervjuu on kindlasti sobilik meetod uurimaks inimeste arusaamu ja tajusid, aga ka teadmisi arvutite ja Internetiga seotud ohtudest. Seda eelkõige seetõttu, et standardiseeritud küsimustikus võivad inimesed anda enda seisukohalt valesid aga ühiskondlikult aktsepteeritud vastuseid, samas kui intervjuus vastutatakse öeldu eest ning intervjuueerijal on võimalik ka juurde küsida ja täpsustada vastaja teadmisi ja arusaamu.

Intervjuust oleks saanud ilmselt rohkem materjali, kui oleks püüdnud arvutitele ja Internetile keskendumisele lisaks uurida ka ületuliselt inimeste tajusid riskidest, eelkõige tehnoloogilistest riskidest, lastes vastajatel ise nende teemade üle arutleda. Samas on selge, et antud uuringu konteksti selline uurimus ei oleks mahtunud, sest küsimusi oli mitmeid ja paljudest erinevatest arvutitega seotud aspektidest. Seega siit järeldus, et edaspidi võiks sellistes intervjuudes keskendudagi ainult ühele teemale, antud juhul ohtudele ja riskidele, ning püüda selle teema võimalikult laialt avada.

Temaatika täielikumaks avamiseks oleks edaspidistes töodes mõttekas uurida AOL ja NCSA kombel inimeste arvamusi, teadmisi ja tajusid ning samal ajal reaalselt olukorda nende arvutites, et ulatuslikumalt kindlaks teha kuivõrd vastuollu need omavahel Eestis lähevad ning kas see on võrreldav Ameerikas saadud tulemustega.

Tuginedes intervjuudest saadud andmetele, võib öelda, et inimesed küll teavad erinevatest arvutite ja Internetiga seotud riskidest, kuid nende teadmised nendega toimetulekust on piiratud. Kui Giddens (1999:3) ütles, et risk viitab võimalusele vältida soovimatuid tagajärgi, siis saadud info põhjal tundub, et inimesed tegelevad arvutitega seotud riskidega siiski pigem alles siis, kui soovimatud tagajärjed on juba käes st viirus arvutis või rämpskirjad postkastis.

Õnneks võib ka kasutada olnud suhteliselt väikese valimi puhul siiski näha positiivseid külgi, kus inimesed vähemasti osade ohtude puhul teavad, mida teha (näiteks oskavad kasutada rämpspostifiltreid) ning seega on teadlikud ja oskavad soovimatuid tagajärgi vältida ehk hoida ära võimaluse nende rämpskirjade avamiseks ja selle kaudu enda arvutisse mõne viiruse, nuhkvara või muu ohtliku programmi tõmbamist.

Samas võib riskiteadlikkuse kohta siiski öelda seda, et vastanud teadsid enamlevinud riskidest, kas selle kaudu, et need on neid ennast puudutanud või selle kaudu, et nad on neist kusagilt kuulnud. Seega ei saa öelda, et arvutite ja Internetiga seotud riskid oleksid inimestele tundmatud ja seeläbi neile ka subjektiivses maailmas olematud. Seda toetab Luptoni (1999: 28-29) väide, et reaalselt ei ole riske olemas, kõik sõltub sellest, kuidas ohtu analüüsida.

Olles ise pigem eksperdi rollis on ka käesoleva töö autoril vastandlikud arvamused arvutite tavakasutajatega, pidades silmas just arvuteid ähvardavaid ohtusid. Lupton (1999: 19-20) kinnitab sama. Intervjuudes rääkisid vastajad enamasti otseselt arvutitega seotud ohtudest ning neis ei keskendunud üldistele ohtudele, mistõttu on hetkel raske kinnitada või ümber lükata Luptoni (1999: 19-20) väidet, et mitte-eksperdid ülehindavad riske, mille kohta saab kergesti infot ning alahindavad neid, mis on üldisemad. Pigem tundub vastustest, et alahinnatakse ka neid riske, mis on lähemal ja millega on kokku puutunud.

Jällegi vastaspoolelt võib tuua antud intervjuudest saadud andmetele tuginedes näiteid, kus inimene, kes arvutiga hoolimatu ümberkäimise tagajärjel kogu arvutis olnud info kaotanud ja arvuti rikki ajanud, tajub seda probleemi lähemana.

Siin võib seoseid näha ka Becki (1992:27) sõnastatud probleemiga, et paljude uute riskide tunnetamine käib inimestele üle jõu ning fookus on aina rohkem nähtamatutel ja tunnetamatutel ohtudel, mis jätab ohvrid ekspertide hinnangute, vigade ja vaidluste meelevalda. Käesoleva töö fookuses olnud ohud on justnimelt enamasti nähtamatud ja tunnetamatud, vähemalt sinnamaani kuni inimene ei ole kaotanud selle tagajärjel midagi olulist, näiteks juba lõppfaasis bakalaureusetööd (sest seda on hoitud ühes eksemplaris ühes arvutis) või pangaarvelt raha (sest masinasse on hooletult sisse lastud nuhkvara).

Usalduse vaatenurgast uuriti vastajatelt nende usaldust internetis oleva info ja sinna enda isikliku info edastamise kohta. Tulemustest kujunes välja kaks vastajagruppi enda kohta info edastamise osas, kellest üks on nõus enda kohta infot edastama valitult ja juhul kui teine pool on piisavalt usaldusväärne (nt pank) ning teine ei ole nõus mitte mingil juhul enda kohta andmeid Interneti edastama.

Internetist saadava info usaldamise osas oli samuti erinevaid arvamusi, millest üks esindab seda poolt, kes üldiselt usaldavad, kuid peamiselt siiski ametlikest kanalitest pärit infot ning muud infot tahaksid kontrollida, ning teised, kes pigem siiski usaldavad sh ka internetisuhtlust. Siingi annab paralleele tõmmata Luhmanni (Luhmann 1988 ref. Giddens 1990:30-31) sõnadega, kes ütleb, et soovimatud tagajärjed on pigem meie enda tegevuste ja otsuste tagajärjed. Vastustest tuli välja seegi, et inimesed, kelle usaldust on korra petetud (nad on saanud Internetist nt mittekehtivad bussiajad), usaldavad vastavalt ka vähem ja on ettevaatlikumad, kui need, kelle usaldust ei ole andmed või Internetisuhtlus jõudnud veel petta.

Giddens (1999:4) on öelnud, et riskiühiskonnas on tegemist teaduse ja tehnoloogia kaudu “toodetud riskidega”. Arvutite puhul kehtib see väide kindlasti, sest mida edasi areneb tehnoloogia ning mida uuemaid tehnoloogilisi lahendusi välja mõeldakse, seda rohkem tekib juurde ka uusi ohuallikaid st igal positiivsel arengul on alati olemas ka varjukülg, kus teisi ära kasutada püüdvad või ebatervelt mõtlevad inimesed leiavad võimaluse mingi ohu luua.

Lähtudes Bloorist (1995: ptk 5 ref. Lupton 1999:21 kaudu), kes ütleb, et riski vältimine on ratsionaalne ja riski võtmine irratsionaalne, võib käesoleva töö raames kogutud tulemuste põhjal väita seda, et inimesed jaotuvad sellel skaalal pigem kusagile keskele, kus osa inimesi tegeleb riskide vähendamisega, kasutades selleks vastavaid programme ja osates neid ise seadistada, teisest küljest on aga inimesi, kes alles probleemi ilmnemisel tegutsevad või paluvad kellegi teise abi.

Kõiki tulemusi vaadates on loomulikult oluline ka inimeste taust, sest kõigilt ei saagi oodata ühtviisi adekvaatseid teadmisi ja oskusi, kui kokkupuuted ja ootused arvutitele ja Internetile on erinevad. Käesoleva töö raames intervjueeritud inimeste taustad varieeruvad vähesest kasutajast mitmekülgsete kasutajateni. Kõigi käesoleva töö raames uuritud aspektide võrdlus näitab, et kasutajate kokkupuudetest ja ootustest tegelikkuses aga paljutki ei sõltu.

Tarkvara seadistamise ning viiruste ja rämpsposti tõrjumise osas ei ole kasutajagruppide vahel erinevusi, samuti on kasutajate usaldus interneti vastu kirjeldatav kui “usalda, aga kontrolli” või mõnel juhul kindlasti ei usaldata, kuid see ei sõltu jällegi sellest, millisesse klastrisse kasutaja kuulub. Arvutiteemalisi artikleid loetakse samuti üle klastrite pigem vähe ja siis, kui teema tundub huvitav.

Üks seaduspära oli aga võrdluse teel võimalik siiski leida – mitmekülgsed kasutajad on need, kes lahendavad arvutiga ettetulevaid probleeme tööl või kodus või nii tööl kui kodus. (*Mitmekülgset infokasutajat iseloomustab informatsioonikeskne internetikasutus. Ta kasutab Interneti majandusliku, rahandusliku, õigusliku ja poliitilise informatsiooni otsimiseks ning õppimise ja erialase tööga seotud infoks* (Runnel & Pruulmann-Vengerfeldt 2004:157))

Toodud seaduspäraga on võimalik seostada ka organisatsiooni taust ehk, millised on infotehnoloogilised reeglid organisatsioonis, kus töötatakse. Kui tööl ei ole kasutajal administraatori õigusi ning kogu süsteem toimib tsentraliseeritult, siis ei ole töö juures tegelikult ka võimalust ise probleeme lahendada. Ühest küljest ei võimalda see kasutajal tõsta riskidega seotud teadlikkust, kuid teisest küljest on organisatsioonile odavam ja mugavam, sest võimaldab olukorda tsentraalselt kontrollida ja arvutid puhtana hoida.

Seega võib öelda, et elame tõepoolest riskiühiskonnas, kus inimesed kõiki ümbritsevaid riske ei taju ega oska näha, sest need on nähtamatud või inimeste jaoks sedavõrd keerulised mõista, et lihtsam on neile mitte mõelda ja neist endale mitte ohtu ette kujutada. Seda nähtamatust ja keerulisust on näha eelkõige just tehnoloogilistes, sh interneti ja arvutitega seotud arendustes, kus kõik on tehtud võimalikult kasutajasõbralikuks, et kasutaja ei peakski teadma neid keerulisi süsteeme, mis selle kasutajasõbralikkuse taga on. Samas, nende süsteemide vähenegi tundmine õpetab ennetama ohtusid, millega täielikus teadmatuses inimene end silmitsi seab.

Arvutikasutajate käitumine on käesoleva töö tulemuste valguses kusagil ratsionaalse ja mitteratsionaalse skaala keskel, kõiki uuritud aspekte ei saa paigutada täpselt skaala samasse punkti, sest üks inimene võib tarkvara lasta seadistada teistel, kuid samas tuleb koduste arvutiprobleemidega ise toime või, vastupidi, ei ole kasutajal tarkvara paigaldamisega probleeme, kuid ise arvutialaste probleemide lahendamisega üldse ei tegele.

Edaspidi soovitab käesoleva töö autor ohtude ja riskide teema uurimisel süveneda kasutajatega selle üle arutlemisse pisut sügavamalt ja laiemalt, sest antud uurimus jäi oma uudsuses ja uurimistingimuste tõttu veidi liiga pinnapealseks, et kõiki aspekte süvitsi tundma õppida.

Kokkuvõte

Käesoleva bakalaureusetöö ülesandeks oli uurida arvutikasutajate riskikäitumist seoses arvutitest ning Internetist tulenevate ohtudega. Alljärgnevalt tuuakse ära vastused uurimisküsimustele ning peamised järeldused.

- Arvuti- ja Internetikasutajate hinnangud oma oskustele: üldiselt ja tarkvara seadistamise osas

Kasutajad hindavad oma oskusi üldises mõõtmises keskmisteks või headeks. Tarkvara seadistamise oskuste osas jagunevad kasutajad järgmiselt: need, kes esmajärjekorras spetsialisti poole pöörduvad, need, kes üritavad probleemiga esialgu ise tegeleda, ning need, kes probleeme ise lahendavad. Viimases grupis jagunevad kasutajad veel omakorda kaheks: täiesti teadlikud ning etteantud juhiste järgi toimijad.

- Arvutite ja Interneti kasutamisel ette tulevate probleemide lahendamine: kes lahendab? Arvuti- ja Internetikasutajate kokkupuuted ja toimetulek viiruste ja rämpspostiga.

Probleemidele lahenduse otsimisel jagunevad kasutajad järgmiselt:

- lahendavad probleeme ise
- probleemid lahendab keegi perekonnast
- probleeme lahendavad sõbrad
- probleeme lahendavad töökaaslased
- probleeme lahendavad organisatsioonis töötavad arvutispetsialistid

Välja joonistuvad ka järgmised grupid:

- Kasutaja lahendab probleemid nii tööl kui kodus
- Kasutaja lahendab probleemid kodus ja tööl teeb seda keegi teine või kasutaja lahendab probleemid tööl ning kodus teeb seda keegi teine
- Kasutaja ei tegele ise üldse probleemide lahendamisega

Rämpsposti ja viirustega on intervjueeritud kasutajatel kõigil kokkupuude olemas, kuid oskused nende vastu võitlemisel on erinevad: on neid, kes oskavad kasutada ja seadistada rämpspostifiltreid ja käivitada viirusetõrjeprogramme, kuid on ka neid, kes on neist võitlemisvõimalustest kuulnud, kuid ise neid seadistada ja kasutada ei oska.

- Usaldus Internetikeskkonna vastu: sinna enda andmete edastamisel ja sealt info kogumisel

Enamiku kasutajate kohta võib öelda, et üldjoontes Internetti sedavõrd ei usalda, et sinna oma isikuandmeid edastada või sealt leitud infot kontrollimata kasutada. On ka neid, kes mitte mingil juhul enda kohta Interneti kaudu infot ei edastaks. Levinum on aga vastanute hulgas põhimõte “usalda, aga kontrolli” – see kehtib nii asutuse kohta, kellele enda kohta infot edastatakse, kui ka info kohta, mida Internetist saadakse.

- Info hankimine meediast arvutitega seotud probleemide kohta: kui aktiivselt loetakse, vaadatakse, kuulatakse? Kui palju meedias arvutiteemalistest ohtudest kirjutatakse?

Üldjoontes võib märkida, et suurem osa kasutajatest loeb arvutite ja internetiga seotud ohtude või üldse teemade kohta käivaid artikleid meedias harva ning vaid siis, kui teema tundub huvitav ja kui sellest aru saadakse. Samas on ka suur hulk (5 vastajat 15st), kes ütlevad kindlalt, et nad arvutiteemalisi artikleid ei loe ning üks, kes loeb artikleid ning vaatab ka arvutiteemalist telesaadet.

Põhilised järeldused kasutatud metoodika osas on seotud materjali kogumise viisiga, kus antud teema edaspidisel uurimisel tuleks kindlasti ohtude teemale keskenduda eraldi, mitte suuremate uuringute raames, sest teemavaldkond on laiem ja sügavam ning nõuaks eraldi käsitlemist.

Peamised järeldused saadud tulemuste osas puudutavad internetikasutaja tüüpi ehk et uuritud aspektid (tarkvara seadistamise ja viiruste-rämpspostiga toimetulek, probleemide lahendamine, usaldus Interneti vastu ja meedias käsitletud ohtude kohta lugemine) ei sõltu kasutaja tüübist ehk klastrist, kuhu kasutaja kuulub, oskused ja kogemused varieeruvad üle klastrite. Üks seaduspära, mis siiski välja koorub, on see, et mitmekülgne infokasutaja tegeleb probleemide lahendamisega tööl, kodus või mõlemas kohas, samas kui teiste kasutajate puhul võib igas klastris leida neid, kes üldse probleemide lahendamisega ise ei tegele.

Oluline järeldus edaspidisteks uuringuteks on ka see, et oluline on probleemide lahendamise puhul lisaks kasutaja tüübile ka organisatsiooni kontekst ja sealsed kokkulepped infotehnoloogiliste küsimuste osas: kas administreerimine on lubatud kõigil

kasutajatel või võivad seda teha vaid infotehnoloogia valdkonna töötajad. Sellest sõltub, kas inimesel on üldse võimalik töö juures probleeme ise lahendada ja seeläbi selle kohta teavet koguda või mitte.

Summary

BEHAVIOR OF COMPUTER AND INTERNET USERS IN RISK SOCIETY

Urmas Rosenberg

The task of current bachelor thesis was to investigate the risk behavior of computer users in situation of dangers created by computers and Internet.

The method used includes mainly interviews with respondents who participated in a study named “Me.World.Media” made by journalism and communication department of Tartu University in 2002 and who had given their positive response to participating in following studies. In the form on pilot research media was also monitored during the two months when interviews were conducted (january and february of 2005).

The results show that interviewees consider themselves quite good or average users of computers and Internet, but at the same time when dealing with software configurations, there are people who turn to a computer specialist at once, people who try to configure programs themselves at first and not so many of those who do it on their own.

When dealing with computer- and internet-related problems, users also can be divided into wider groups: users, who deal with problems at work and at home, users who deal with problems either at work or at home and somebody else deals with problems in the other place and users, who do not deal with problem solving at all.

All respondents have come in contact with viruses and spam, at the same time not all of them can deal with those problems. Some are familiar with anti-virus software and spam-filters and can use and configure them on their own, others know that this software and these filters exist, but do not know how to configure them or use them.

When talking about trust towards Internet – receiving data from there and giving out personal information –, then the most common principle is to trust, but verify. Principle that applies as well as to organisations who ask certain personal information, as to information received from Internet.

It can be said, that most users read rarely articles or watch TV shows or listen to radio shows, only when theme seems interesting enough and it is understandable for him/her.

Main conclusion about collecting data is that when researching into the subject further it will be more handy to concentrate in interviews solely on risk theme and not make the inquiry as a part of a bigger study, because the subject is deeper and wider and requires separate inquiry.

Result-wise it is important to note that the clusters where users belong to, did not matter much in a current study. It did not depend on what kind of a user is dealt with when talking about his/her skills in configuring software or trusting Internet. There was one legality though – a versatile information user deals with computer-related problem solving either at work or at home or at both places, when in all other clusters those users can be found who do not deal with problem solving at all.

It is also important to research further into the context at work, mostly about rules in IT department – whether all computers are administrated only by IT people or all people are administrators of their computers.

Kasutatud kirjandus

- Lupton, D. (1999). Risk. London: Routledge.
- Beck, U. (1992). Risk Society, Towards a New Modernity. London : SAGE Publications Ltd.
- Giddens, A. (1999), Risk and Responsibility. The Modern Law Review, 62 (1999), 1, 1-10.
- Giddens, A. (1990). The Consequences of Modernity. California : Stanford University Press
- Vengerfeldt, P., Runnel, P. (2004). Uus Meedia Eestis. Meediasüsteem ja meediakasutus Eestis 1965-2004. Vihalemm, P. Tartu: Tartu Ülikooli Kirjastus, 233-256.
- Runnel, P., Pruulmann-Vengerfeldt, P. (2004). Mobiilid, arvutid, internetid: Eesti Infoühiskonna Künnisel. Eesti elavik 21. sajandi algul. Kalmus, V., Lauristin, M., Pruulmann-Vengerfeldt, P. Tartu: Tartu Ülikooli kirjastus, 147-162.
- Van Loon, J. (2002). Risk and Technological Culture. Towards a sociology of virulence. London : Routledge.
- AOL/NCSA Online Safety Study
http://www.staysafeonline.info/news/safety_study_v04.pdf. Vaadatud 2005.04.27
- Kendra, M. A., George, V.D. (2001). Defining Risk in Home Visiting. Public Health Nursing, 18, 2, 128-137
- Anto Veldre, Turvalisuse kolm põhikategooriat. (2003). <http://www.am.ee/6550> vaadatud 2005.05.20
- Neumann, P. (1995) Computer-Related Risks. ACM Press / Addison Wesley
- Alberts, C., Dorofee, A. (1992) Managing Information Security Risks. The OCTAVE Approach. Boston: Addison Wesley Professional.
- Internetti kasutab 51% 15-74-aastast eesti elanikest. (2005).
<http://www.emor.ee/arhiiv.html?id=1322> , mai, 2005

Lisa 1 – Internetikasutajate intervjuu kava

Valdkonnad, eesmärgid:

I Sotsiaalne võrgustik, kodu, sõbrad, õppimine, töö, huvid ja harrastused

II Arvutid ja Internet: Kogemused, ootused, harjumused, hüved, hoiakud, motivatsioon

III Internet ja sotsiaalne võrgustik, suhtlemine

IV Info otsimine

V Tarkvara ja riistvara: hirmud, oskused

VI Info ja kommunikatsioon, infoühiskond (mõiste tähendus, kokkupuude sellega),

SISSEJUHATUS

Te osalesite kaks aastat tagasi üle-eestilises uuringus Mina. Maailm. Meedia, mis käsitles teie elu, harjumusi ja eelistusi ning detailsemalt meedia tarbimist ning Interneti ja arvutite kasutamist. Te andsite nõusoleku vastata sama uuringu raames veel mõnele küsimusele. Kas teile meeldis selles uuringus osaleda? Kuivõrd teile meeldis oma elu ning maailmavaadet sellise küsitluse kaudu jälgida?

I Sotsiaalne võrgustik, kodu, sõbrad, õppimine, töö, huvid ja harrastused

Praeguse intervjuu eesmärgiks on rääkida pisut veelgi põhjalikumalt meedia ja arvutite ja interneti osast teie elus ning tegemistes ja teie üldisest suhtumisest nendesse tehnoloogiatesse.

Esmalt palun rääkige meile pisut oma elust üldiselt!

1. Mis valdkonnas te praegu tegutsete/töötate või õpite?

1.2 Olete te viimase kümne aasta jooksul eriala või töökohta vahetanud? Mis põhjusel?

2. Kuivõrd peate te oma praegust elu huvitavaks ja õnnelikuks; raskeks ja nõudlikuks; võimalusterohkeks; rutiinseks (palun tooge näiteid).

2.1Kuidas teile tundub, millest teie eluga rahulolu ning tegevustega toimetulek kõige enam sõltub?

2.2Oskaksite ja tahaksite te nimetada mingeid olulisi asjaolusid, mis seavad teie elule piiranguid või mingeid asjaolusid, mis on rahulolu, eesmärkide saavutamisel ja eluga toimetulekul eriti olulised?

3. On teil aega väljaspool tööd ja pereelu ka huvialadeks või nn vaba-aja harrastusteks? Millised need on?

3.1 Meeldib teile raamatuid lugeda, reisida, teha käsitööd või pildistada-filמידa, vaadata filme, sportida, tehnikaga tegeleda, aiandusega tegleda, kinos, teatris või kontserdil käia, ringides või koorides osaleda, ise midagi kirjutada, sõpradega aega veeta vms?

3.2 Kas te reisite? Kas töö või puhkuse eesmärgil? Kus?

3.3 Kui oluline on teie elus töö võrreldes vaba aja harrastustega?

3.4 Kas harrastused on teil isiklikud, või tegelete te oma huvialaga kellegagi koos (perega, sõpradega?)

4. Milline on teie igapäevaelus sõprade-tuttavate osa?

- 4.1 Kas suhtlete nendega tihedalt, igapäevaselt või pigem harva?
- 4.2 Kuivõrd te arutate nendega oma elu, perekonda puudutavaid asju?
- 4.3 Kuivõrd palju on teie sõbrad seotud teie huvialade ja harrastustega?
- 4.4 Kuivõrd arutate nendega maailma ja Eesti asju?
- 4.5 Kuivõrd oluliseks infoallikaks ja nõuandjaks te neid peate?
- 4.6 Arvestate te nende arvamusega?

5. Kuidas te oma elutempot iseloomustaksite?

- 5.1 On teil vahel kiire? Mis seda põhjustab?
- 5.2 Kuidas teil õnnestub aega kokku hoida?
- 5.3 On teil vahel igav? Kuidas te igavust peletate?

6. Kas teile meeldib end täiendada? (õppida, maailma asjadest teada saada, infot koguda, ülesandeid lahendada)?

- 6.1 On teil selleks elus või töö tõttu otseseid vajadusi?

II Arvutid ja Internet:

Kogemused, ootused, harjumused, hüved, hoiakud, motivatsioon

Internet on inimeste elus muutunud tihti üsna igapäevaseks ja nii on isegi raske öelda, kui oluline on selle osa. Meid huvitab siiski, kas, mis põhjustel ja kuidas teie ning teie sõbrad-tuttavad eelkõige Internetti kasutavad. Esmalt mõned üldised küsimused, millest pärast räägiksime ka pisut põhjalikumalt.

1. Mäletate te, kes teie sõpruskonnas hakkas Internetti kasutama esimeste hulgas, kes viimastena?

- 1.1 On teie tutvuskonnas või perekonnas neid, kes Internetti ei kasuta?
- 1.2 Kes sõpruskonnas hakkas varem, kes hiljem netti kasutama?
- 1.3 Kuivõrd lihtne oli teile endale arvutite ja interneti kasutamine? Õppisite te seda eraldi? Kelle käest? Kus? Kuivõrd oskajaks te ennast ise võrreldes teistega peate?
- 1.4 Kuivõrd sõltub interneti kasutamine teie arvates vanusest, haridusest, sotsiaalsest staatusest või muust sellisest? Millised inimesed Internetti kõige enam kasutavad? Oskate te oma tutvuskonna põhjal näiteid tuua?
- 1.5 On teil tähelepanekuid ka selle kohta, milleks teie sõbrad, tuttavad, pereliikmed kõige enam arvuteid ja Internetti kasutavad?

2. Mis eesmärgil te kõigepealt Internetti kasutama hakkasite?

- 2.1 Mida sealt otsisite või leida lootsite? On see tänapäeval kuidagi muutunud?
- 2.1 Mis te arvate, kas inimesed on oma harjumusi Internetiga seoses kuidagi muutnud? Aga teie ise?

3. Kui palju aega kulub teil umbes keskmisel päeval Interneti kasutamisele?

4. Oskate te nimetada oma elus mingeid valdkondi, kus võite öelda, et Internet on teile kasulik?

- 4.1 Kas oskate tuua mingeid näiteid?

(KUI ei oska, SIIS abiküsimusteks: Mis tüüpi olukorraga on tegu – info otsimine, inimestega suhtlemine (tööalane, eraeluline?), probleemi, lahenduse otsimine (mis

valdkonnas see oli: töö, isiklik elu, suhted, tervis. Kas tahate tuua mõnda näidet)?

4.2 Milleks te seda kasutate?

(abiküsimused: e-mail, ajalehtede-ajakirjadne lugemine, infootsing, eraelulised teenused, ajaviide, arvamuse avaldamine. Vastavatel teemadel eraldi rääkimine sõltuvalt toodud näidetest)

5. Kuivõrd on Internet teile vaba aja veetmise vahend?

(abiküsimused: netis surfamine? Hobide kohta info otsimine? Mängud? Rate ja muud sellised suhtluskanalid? kohtamisteenused?)

6. Olete te internetipanga kasutaja?

7. Olete te Interneti vahendusel midagi ostnud?

7.1 Aga Internetis näiteks hindu võrrelnud?

7.2 Kui olete teinud oste, siis kas teete ostu kohe, või vaatate kaupu mitu korda?

7.3 Mis laadi oste olete Internetis teinud – kas eesti e-poodidest või välismaalt?

7.4 Mis eelised on Internetist ostmisel poest ostmise ees?

8. Kuivõrd oskate te hinnata oma harjumusi üldiselt: kasutate te rohkem kindlaid lehekülgi või varieeruvad leheküljed, te internetis külastate, palju? Millega see on seotud?

III Internet ja sotsiaalne võrgustik, suhtlemine

1. Milliste suhtluskanalite abil hoiate kontakti oma sõprade-tuttavatega? (mobiil, telefon, näost näkku suhtlemine, sms, internet – e-post, MSN, jutukas, Skype, mingid muud online-suhtlusvahendid? Millised?)

1.2 Oskate te hinnata, millest just nende suhtlemisvahendite kasutamine?

1.3 Milline kanal/vahend on teile kõige meelepärasem?

3. Kuivõrd palju külastate te ise mitmesuguseid foorumeid, suhtlete interneti vahendusel võõraste inimestega?

3.1 On see rohekm üldine arvamuse avaldamine, või on teil ka isiklikke tutvusi?

3.2 Milliseid foorumeid te külastate?

4. Kuivõrd te Internetisuhtlust usaldate? On teid Internetis ninapidi veetud või olete ise kellegagi nalja teinud?

5. Kas suhtlemine Internetis on teie jaoks kuidagi erinev suhtlemisest reaalses elus? (abiküsimused: kas olete netis suheldes julgem, avatum, enesekindlam või vastupidi?)

5.1 Olete te märganud erinevusi näiteks lähedaste tuttavate interneti- ja tavaelu käitumist võrreldes?)

6. Kuivõrd te jälgite ajalehekommentaare või külastate suhtluslehekülgi, ajaviiteportaale, erialaportaale või uudisgruppe?

7. Kas te olete saanud foorumite/jututubade/ajalehekommentaariumide kaudu ka teile kasulikku infot (eluaseme, töö, tervise vms) kohta?

7.1 Kas te usaldate sellisel teel saadud infot ja kui palju?

7.2 Kas te kontrollite kuidagi selle usaldusväärsust? Kuivõrd selle kontrollimine on

oluline?

8. Olete te kokku puutunud üle Internetis toimuvate mängudega?

8. Mida te arvate, miks kasutavad inimesed selliseid suhtlusvõimalusi nagu rate.ee või orkut.com? Teevad isiklikke kodulehekülgi?

8.1 Kuidas te neisse portaalidesse suhtute? Kuidas te suhtute näiteks Delfi portaali või ajalehtede kommentaarikeskustesse?

8.2 Kuivõrd peegeldavad Internetis leiduvad kommentaarid avalikku arvamust? Mis laadi teemade juures tunnete kõige rohkem huvi teiste lugejate arvamuse vastu ehk netikommentaari vastu?

9. Kas foorumid, kogukonnad, internetikommentaarid jms, kus te osalete, on mõjutanud või mõjutavad teie hoiakuid?

9.1 Kui tugevalt tunnete end olevat seotud nende gruppidega, kuhu te kuulute?

9.2 Kas grupp ja selle vaated mõjutavad või on mõjutanud teie hoiakuid?

9.3 Kas külastate ka neid foorumeid, mille põhimõtted ei lähe otseselt kokku teie omadega? Mis eesmärkidel?

10. Loete te mingeid liste? On need seotud teie tööga, teie huvialadega, või on sõpruskonna- perekonna privaatsed listid?

10.1 Kas need on rohkem info jagamise ja teadaannetega seotud, või käib seal listi liikmete vahelisi arutelusid?

11. Olete te Internetis tutvunud uute inimestega?

11.1 Mis tasemele need tutvused on arenenud?

11.2 Kuivõrd on Internetis võimalik heade või lähedaste suhete tekkimine?

IV Info otsimine

1. Kuivõrd tihti kasutate te Interneti millegi teada saamiseks, mingi info leidmiseks?

1.1 Oskate te tuua näiteid viimase nädala kohta – mis valdkondades olete infot otsinud?

1.2. Küsida kõigi valdkondade kohta: olete te otsinud/kasutanud/vaadanud uudiseid, eluasemega, tööga, reisimisega, kohtamisteenustega seotud infot, perega, tervisega seotud infot, hobidega seotud, seaduseid ja õiguslast infot vms?

1.3 Oskate te öelda, kuivõrd oluline infoallikas Internet teile on? Kas te kasutate ka muid infoallikaid: käite raamatukogus, helistate infotelefonidele, kasutate teatmeteoseid ja sõnaraamatuid?

1.4 Kuivõrd on Internet muutnud teie infootsimisharjumusi?

2. Kas te olete ka ise Interneti vahendusel püüdnud infot pakkuda, levitada? Mis valdkonnaga see on seotud?

2.1 Kuivõrd te usaldate Internetti? Olete te Interneti vahendusel oma andmeid edastanud? Millega seoses (krediitkaarditehingud nt)?

2.2 Kas annaksite Internetti oma isiklike andmeid?

3. Millistes eluvaldkondades või teemadel on info otsimine Internetist hea ja mugav?

3.1 Kuivõrd võib öelda, et leiate Internetist infot, mis teie elu kuidagi paremaks (mitte

tööga seotud asjad: reisimine, pere ja tervisega seotud info, kohtamisteenused jms)?
Meenub teile mõni näide?

4. Kuivõrd te olete Internetti kasutanud enda elu paremaks muutmiseks?

4.1 Olete te näiteks ostnud, müünud või rentinud eluaset?

4.2 Otsinud tööd?

4.3 Otsinud infot seoses reisile minekuga/korraldanud kavandatava reisiga seotut?

4.4 Otsinud meditsiinilist infot?

4.5 Oskate te tuua mõnd näidet, kuidas see on teie elu paremaks teinud?

5. Kuidas te Internetist infot otsite?

5.1 Otsite te mingeid kindlaid lehekülgi? Surfate niisama?

5.2 Kuivõrd on teil vajaliku info leidmiseks abi otsimootoritest?

5.3 Kuidas te oma oskusi Internetist info leidmisel hindate? On info leidmine sealt lihtne või keeruline?

6. Milliseid sisulisi takistusi on teil Internetist info otsimisel ette tulnud?

6.3 Milliseid lehekülgi, portaale vms te info leidmiseks kasutate?

6.4 Kuidas teile tundub – kas olete Internetist saadava infohulgaga rahul, on seda liiga palju või liiga vähe? Miks teile nii tundub? Kui palju vaeva nõuab soovitud asja leidmine?

7. Kuivõrd kasutate eestikeelseid ning kuivõrd võõrkeelseid netilehekülgi? Miks?

7.1 Kas mõne keele mitte tundmine on olnud takistus soovitud info omandamisel, (kas vastaja on kasutanud Internetis tõlkimisteenuseid?)

7.2 Mis keeles lehekülgi te kõige enam kasutate?

8. Kui te leiate Internetist midagi huvitavat, kuidas käitute? Kas otsite teema kohta infot juurde või jätate selle sinnapaika?

V Tarkvara ja riistvara: hirmud, oskused

Meil on mõned küsimused ka Interneti ja arvutite hooldamise ja nendega seotud probleemide kohta.

1. Kuivõrd oskajaks arvutikasutajaks te end peate? On see viimase paari aastaga muutunud?

2. Kuivõrd hästi valdate enda hinnangul neid programme, mida teil igapäevases tegevuses kõige enam vaja läheb (nt tekstitöötlusprogrammid, pilditöötlusprogrammid, tabelarvutusprogrammid jms?)

3. Kuivõrd oskajaks peate ennast

3.1 vajaliku tarkvara leidmisel, installeerimisel, vajadusel eemaldamisel või kaasajastamisel,

3.2 võrguühenduse konfigureerimises,

3.3 kodulehekülje või esitluste tegemises?

4. On teil olnud kogemusi viiruste, rämsposti vms ebameeldivustega? Oskate te viiruste, spämmi jms kaitseks midagi ette võtta? Mida näiteks?

(Urmase selgitus: tundmatuid kirju ei loe, attachmente ei ava, töö mail ainult töö jaoks jne?)

5. Kui teie arvuti töös tuleb ette tõrkeid, kas oskate neid ise lahendada või pöördate asjatundjate poole? Mis tüüpi probleemidega on enamasti tegu olnud?

6. Kas ise aitate või juhendate teisi arvuti kasutamisel?

6.1 Kui teil on kodus arvuti, siis kes enamasti lahendab arvuti hooldamisega seotud küsimusi?

7. Kust veel leiate abi probleemide lahendamisel?

7.1 Kuivõrd jälgite arvuti probleemidega seotut ajakirjandusest? Oskate nimetada ajakirjandusväljaandeid, kus neist kirjutatakse/räägitakse? Kui näiteks näete arvutitega seotud lugusid päevalehtedes, kas vaatate neid või liigute edasi?

VI Info ja kommunikatsioon, infoühiskond (mõiste tähendus, kokkupuude sellega), poliitika, globaalne areng, üldised hüved

1. Oskate te nimetada mingeid Internetist kättesaadavaid teenuseid, millest teile kasu on olnud?

1.2 Näiteks Eestis pakutavad avaliku sektori teenused, pangateenused, bussiinfo, ja palju muud või Internetis üldiselt pakutavaid? (kuni meilboksi tulevate spämmkirjade ravimipakkumiseni välja)

1.3 Millistest teenustest puudust tunnete?

2. Olete te kasutanud Internetti kohaliku omavalitsusega suhtlemisel?

2.1 Milliseid teenuseid võiks näiteks Tartu linnavalitsus Interneti vahendusel pakkuda?

3. Kuidas teile tundub, kuivõrd arvestatakse Eestis e-teenuste väljaarendamisel Internetikasutajatega, kuivõrd neilt küsitakse nõu? Kas olete ise aidaund kaasa mõne e-teenuse arendamisel, kuivõrd oleksite valmis kaasa lööma? Milles kaasaitamine võiks seisneda?

2 Milline on teie arvates infotehnoloogiliste teenuste tulevik Eestis lähematel aastatel?

4. Jälgite te arvutite ja Interneti kajastamist meedias?

4.1 Kui, siis miks? Milliseid teemasid? Nimetage mingeid meelde jäänud teemasid?

5. On teil ID kaart? Kuivõrd head on teie arvates selle praegused kasutamismõimalused? Olete te seda kasutanud? Kas te osaleksite e-valimistel?

6. Oskate te nimetada mingeid huvitavamaid või silmapaistvamaid E-arenguid Eestis?

6.1 Kuivõrd palju neist üldse teatakse?

7. Praegusel ajal kasutatakse mõisteid infoühiskond ja teadmushiskond. Neile antakse mitmeid erinevaid tähendusi.

7.1. Mis te arvate, kas teie kuulute infoühiskonda? Kas teie tegevusala on iseloomulik infoühiskonnale? Miks?

7.2 . Kuivõrd on Eestis infoühiskonna arengukavad teie arvates seotud inimeste igapäevaeluga?

8. Kuivõrd te sõltute tehnoloogiast nagu mobiil ja Internet? Kuivõrd sõltub tänapäevane ühiskond tehnikast või kuivõrd on see sõltuvus illusoorne?

Täname meiega oma mõtteid jagamast!

Taru Ülikooli Ajakirjanduse ja Kommunikatsiooni Osakond

Lisa 2 – Intervjuude läbiviimise tabel

Intervjueerija	Intervjueeritav	Tegevusala	Amet	Koht	Kestvus
Kristiina	M4 = 24 a	arstiteadus	töötav tudeng	Tartu	62 min.
Tagel	M6 = 19 a	metalli eriala	meistri abi	Tartu	44 min.
	M5 = 20 a	ehitus	töötav tudeng	Tartu	59 min.
	N7 = 27 a	bioloogia	lapsega kodus	Tartu	80 min.
Marko	N6 = 39 a	poliitika	ametnik	Tallinn	59 min.
Paloveer	N5 = 25 a	halduskorraldus	tudeng	Tallinn	106 min.
	M3 = 60 a	haridus	koolijuht	Tartu	82 min.
	N4 = 59 a	telefonivõrk	pensionär	Tallinn	81 min.
Piret	N9 = 22 a	sotsiaaltöö	töötav tudeng	Tallinn	98 min.
Reiljan	N3 = 39 a	majandus	analüütik	Tallinn	86 min.
	M7 = 25 a	meelelahutus	baarman	Tartu	72 min.
	N2 = 50 a	psühholoogia	vabakutseline	Tallinn	69 min.
Urmas	N1 = 31 a	põllumajandus	riigiametnik	Tartu	65 min.
Rosenberg	N8 = 42 a	käsitöö	FIE	Tartu	60 min.
	M2 = 26 a	ettevõtlus	töötav tudeng	Tartu	72 min.
	M1 = 48 a	põllumajandus	jurist	Tartu	54 min.
					1149 min.
				Kokku:	~ 19 tundi

M = Mees

N = Naine

Lisa 3 – Eesti Päevalehe ja Postimehe monitooring perioodil 01.01.05 – 28.02.05

Eesti Päevaleht, 2005

Jaauuar. Kokku 25 ajalehte

	<i>Kuup</i>	<i>Vorm</i>	<i>Ma ht</i>	<i>Lk</i>	<i>Pealkiri</i>	<i>Sisu kommentaär</i>
1	4.1.05	Uudis	1/2	13	Netis piraatluse levitajate elu läheb kibe	Hoiatus, et hakatakse rohkem kontrollima, jäljed jäävad alati ning et karistused on suured
2	4.1.05	Uudis	4/5	10		Marsi kulguritest
3	6.1.05	Uudis	1/2	13	Failivahetuse kasutajad satuvad löögi alla	Mida võib, mida mitte, õpetus
4	12.1.05	Uudis	1/2	11	Ärileht: Arvutikaupade hinnad langevad	Mida rohkem müüakse, mis populaarsem..
5	13.1.05	Uudis	1/1	17	Veebilehel saab sõlmida 100 aastat kestvaid kihlvedusid	
6	14.1.05	Uudis	2/5	17	Mobiilipetturid koguvad kõnedega boonusaega	
7	15.1.05	Uudis	1/2	5	Kurikael lavastas firma juhtide kirjavahetuse	Mis võib juhtuda kui varastatakse identiteet.
8	15.1.05	Uudis	1/1	20	Kaks eesti meest tegid maailmas ainulaadse projekti	Mobiiliga linnaliikluse jälgimine
9					Võrku pandi üles natsismi ülistav leht	?
10	16.1.05	Lühieuudis	1/6	22	Eesti populaarseim veebikeskond neti.ee läbis ilukuuri	

	<i>Kuup</i>	<i>Vorm</i>	<i>Mah</i> <i>ht</i>	<i>Lk</i>	<i>Pealkiri</i>	<i>Sisu</i> <i>kommentaar</i>
11	19.1.0 5	Uudis	1/2	5	Arvutiprogramm ennustab hitte	Loodi mingi arvutiprogramm mis oskab öelda kui edukas lugu saab olema
12	21.1.0 5	Uudis	1/2	13	Pätid püüavad lihtsameelsetelt internetipanga paroolle välja petta	Kui palju juhtumeid on, mis moodi toimuvad. Hästi natuke juttu ka keyloggeritest
13	22.1.0 5	Uudis	1/1	24	Apple tegi PC kasutajatele pisikese üllatuse	Katse meelitada inimesi Mac'i juurde
14	24.1.0 5	Uudis	4/5	15	Maailma suurim veebientsoklüpeedia	Wikipedia
15	25.1.0 5	Uudis	1/6	9	E-hääletus annab võimaluse oma valikut muuta	

Veebruar. Kokku 23 ajalehte.

	<i>Kuup</i>	<i>Vorm</i>	<i>Mah</i> <i>t</i>	<i>Lk</i>	<i>Pealkiri</i>	<i>Sisu</i> <i>kommentaar</i>
16	1.2.05	Uudis	2/5	18	Metaotsingu mootorid on muutunud visuaalsemaks	Võrreldakse omavahel.
17	2.2.05	Arvustus	1/4	22	Venelased valavad oma häbi Delfi kommentaaridesse	
18	19.2.0 5	Uudis	1/2	21	Õhukeste monitoride pealetund	
19	23.2.0 5	Uudis	2/5	15	Ärileht: Eestlased töid turule maailmas ainulaase teenuse	Broneeringud internetis
20	28.2.0 5	Uudis	2/3	21	CV sisestamine on liiga keeruline	Võrreldakse omavahel kolme suuremat portaali. Tegu reklaamuudisega

Postimees, 2005

Jaanuar. Kokku 25 lehte

	<i>Kuup</i>	<i>Vorm</i>	<i>Maht</i>	<i>Lk</i>	<i>Pealkiri</i>	<i>Sisu kommentaar</i>
21	3.1.05	Uudisnupp		24	Soome teed digitaliseeritud	Soome kaardistas 430000km teid, abiks tuletõrjele ja päästeametile
22	4.1.05	Uudis	1/2	8	Moobilikliendid käivitusid loiult	Numbriliikuvuse kohta
23	6.1.05	Uudis	1/2	27	Mobiilisulid petavad heausklikelt võltssõnumitega raha välja	Sms – auto katki, saada raha jne
24	7.1.05	Uudis	1/10	8	Korea insenerid ehitasid õppimisvõimelise roboti	
25	7.1.05	Uudis	2/5	3	Rahapuudus viis veebist tasuta sõnaraamatud	
26	11.1.05	Lugejakiri	1/7	13	Keeleveeb ristsõnalahendajate abimehena	Kurvastab, et keeleveeb tasuliseks muutus
27	13.1.05	Uudis	1/2	25	Mobiilifirmade peibutistes peituvad konksud	
28	19.1.05	Uudis	4/5	26	Mööbli saab koju ka arvuti eest lahkumata	Reklaam. Võrreldakse omavahel online mööblipoode
29	24.1.05	Uudis	1/4	23	Arvutimüük pidurdub	Suurfirmade müüginumbrid
30	24.1.05	Uudis	~1/4	23	Fotosid saab tasuta internetis hoida	Picasa, Google
31	24.1.05	Uudis	1/8	23	Aasta lõpuks 2 miljardit mobiilikasutajat	

Veebruar.

	<i>Kuup</i>	<i>Vorm</i>	<i>Maht</i>	<i>Lk</i>	<i>Pealkiri</i>	<i>Sisu kommentaar</i>
32	1.2.05	Uudis	1/1	8	E-valimine võib saada tõelise tuleproovi sügisel	

	<i>Kuup</i>	<i>Vorm</i>	<i>Maht</i>	<i>Lk</i>	<i>Pealkiri</i>	<i>Sisu kommentaar</i>
33	2.2.05	Uudis	4/5	28	Kodune internet juhtmevabaks	Lihtne ja selge õpetus kuidas paigaldada WiFi ruuter. Hinnad. Turva
34	7.2.05	Uudis	4/5	4	Vene mõjukam IT-guru soovib Eesti uuendusi ida poole müüa.	Vene turg on suur ja lai
35	8.2.05	Uudis	3/5	5	Ülikoolitaotlusi saab tänavu esitada veebis	Uudis tegelikult sellekohta, et seda infosüsteemi hakatakse looma?
36	14.2.05	Uudis	1/4	28	Mobiiltelefonide vahendusel teleprogramme veel vaadata ei saa	
37	21.2.05	Uudis	2/5	28	X-Box'i mängukonsoolide juhtmed võivad põleda	
38	21.2.05	Uudis	1/2	9	Sülearvutite menu kasvab	
39	28.2.05	Uudis	1/5	24	Digitaalne lõhe eristab rikkaid ja vaeseid	Arengumaade võrdlus..
41	28.2.05	Uudis	1/8	24	Rämpsposti vastu võitlemine neelab igal aastal miljardeid kroone	Jutt ainult numbritest ja kulutustest